جامعة قاصدي مرباح – ورقلة

كلية الحقوق و العلوم السياسية

قسم العلوم السياسية

مذكرة تخرج لاستكمال متطلبات لنيل شهادة الماستر في ميدان الحقوق والعلوم السياسية

الشعبة: علاقات دولية

التخصص: دراسات أمنية و استراتيجية

بعنوان:

استخدام القرصنة الإلكترونية في السياسة الروسية
(بين التجريم الدولي و حتمية التخابر)

إعداد الطالب: مهني محمد شرف الدين

إشراف الدكتور: بن الشيخ عصام

أعضاء لجنة المناقشة	
الصفة	إسم ولقب الأستاذ (الرتبة العلمية)
رئيسا	– عبد الكريم باسماعيل
مشرفا ومقررا	– عصام بن الشيخ
مناقشا	– فريدة طاجين

نوقشت وأجيزت يوم :2018/06/07

السنة الجامعية: 2017–2018

جامعة قاصدي مرباح – ورقلة

كلية الحقوق و العلوم السياسية

قسم العلوم السياسية

مذكرة تخرج لاستكمال متطلبات لنيل شهادة الماستر في ميدان الحقوق والعلوم السياسية

الشعبة: علاقات دولية

التخصص: دراسات أمنية و استراتيجية

بعنوان:

استخدام القرصنة الإلكترونية في السياسة الروسية بين التجريم الدولي و حتمية التخابر

إعداد الطالب: مهني محمد شرف الدين

إشراف الدكتور: بن الشيخ عصام

أعضاء لجنة المناقشة	
الصفة	إسم ولقب الأستاذ (الرتبة العلمية)
رئيسا	– الدكتور : بن الشيخ عصام
مشرفا ومقررا	
مناقشا	

نوقشت وأجيزت يوم :..../2018/06

السنة الجامعية: 2017-2018

بسم الله الرحمان الرحيم

﴿وتَعَاوَنُوا عَلَى الْبِرِّ وَالتَّقْوَى وَلَا تعَاوَنُوا عَلَى الْإِثْمِ وَالْعُدْوَانِ﴾.

صدق الله العظيم (سورة المائدة: الآية 2)

الإهـــــــداء

" الحمد لله كثيرا على إنعامه وأكملا "

إنه لمن دواعي السرور أن يصل الإنسان إلى مبتغاه الذي طالما كافح وجاهد من أجله وسهر الليالي الطوال في سبيل تحقيقه ، أهدي ثمرة عملي إلى التي رفع الله من مقامها وجعل الجنة تحت أقدامها إلى التي غمرتني بعطفها وحنانها و حبها .... صاحبة القلب الواسع، صاحبة الفضل التي مهما فعلت وقلت لا أوفيها حقها، أنا بدوري أهدي ثمار جهدي إلى أعز وأحن أم في الدنيا التي غمرتني بحبها وحنانها ولم تبخل علي بدعواتها وبركاتها التي لا ترقى لوصفها قواميس فكري.

إلى رمز الحب والعطاء والوفاء

إلى من ربتني بلطف ومنحتني الحنان

إلى تلك المرأة العظيمة التي علمتني معنى الحياة

إلـــى قـــرة العيـــن.

" أمي العزيزة الغالية حفظها الله تعالى "

* * *

إلى من تعجز السطور والكلمات عن الإمتنان له ، و إلى الدي ألهمني روح القوة والمثابرة وعلمني معنى التحدي أمام الصعاب وقهر الظروف والمحن أبي الغالي

الذي علمني لغة القلم واستسقيت منه شعلة العلم التي أنارت دربي وجعلتني أرتادآفاق المعرفة وانهل من بحوره العميقة أبي

أهدي لك تلك الكلمات، بكل المعاني و الوفاء أتقدم بالشكر الجزيل

"أبي العزيز حفظه الله تعالى "

إلى أخواتي الذين بفضلهم قهروا الظروف والمحن لإهداء بسمة الأمل و سندا لي في كل حياتي ، شمعه تنير ظلمة حياتي

إلى من بوجودهم أكتسب قوة و محبة لا حدود لها إلى أحن أخوات عندي في الدنيا

" أحـــــــــلام، منـــــــــــى، وداد، إنصـــــاف "

إلى اللذين استلهمت منهم العفوية والبراءة

وخاصة عمي" كافي محمد "

وخاصة " بن علي عمر شابحة " قامت بمساعدتي كثيرا في هاته الدراسة افادتني حقا بمراجع كثيرة، من جامعة برياطانيا و كل الشكر و الفضل ، شكرا "شابحة "

وإلى كل طلبة العلوم السياسية

كما أهدي إلى من جمعني معهم مشوار دراستي و من حملت معهم لواء الصداقة وألفت فيهم طريق الرشد ، وإلى كل من يعرفني.

وصفوة القول قوله تعالى:

«يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ»

" مـهـنــــــــي محمــــــــــــد شـــــــرف الـــــديــــــن"

شكر و تقدير

إن الشكر لله رب العالمين الذي خلق وهدى وخرج هذا العمل بعون وتوفيق منه نحمده ونشكره وفقنا وأنعم علينا بنعمته وأكرمنا بفضله وعطائه وأمدنا بالقوة وألهمنا هبة الصبر لإنجاز هدا العمل المتواضع.

***

ثم الفضل والشكر والثناء إلى من امتدت يديه فيما أنجزته توجيها ومراجعة منه وتمحيصا وإشرافا الى

أستاذي الكريم الذي لم يبخل علي بنصائحه وتوجيهاته القيمة طوال فترة البحث فجزاه الله خيرا وأطال عمره.

الدكتور " بن الشيخ عصام" حفظه الله

كما نتوجه بالشكر إلى كل من ساعدني في إنجاز هدا البحث في نصحي وتشجيعي ومساعدتي ولو بكلمة طيبة من قريب أو بعيد.

إلى كافة أساتذة العلوم السياسية بجامعة قاصدي مرباح بورقلة على المعرفة التي قدموها لي.

وأرجو من الله أن يجعل هدا العمل خالصا لوجهه الكريم وأن يجعل ثوابه في ميزان حسناتنا.

خطة البحث

استخدام القرصنة الإلكترونية في السياسة الروسية:(بين التجريم الدولي وحتمية التخابر)

مقدمة

الفصل الأول: ماهية القرصنة و طرق منعها

- المبحث الأول: ماهية القرصنة و الحروب السيبرانية

- المبحث الثاني: دور القانون الدولي في تجريم القرصنة و الحروب السيبرانية.

- المبحث الثالث: ظاهرة ويكليكس و القرصنة الروسية للإنتخابات الأمركية الأخيرة.

الفصل الثاني: الصراع الدولي الأمريكي و سلاح الأنترنت

- المبحث الأول: الصراع على الهيمنة بين (الولايات المتحدة الأمريكية - وروسيا

- المبحث الثاني:تجربة القرصنة الروسية و الكورية نموذجا (Sony) .

- المبحث الثالث: القرصنة الروسية في الإنتخابات الرئاسية الأمريكية

الفصل الثالث: مشكلات و عيوب القرصنة و علاقتها بالعمل الإستخباراتي

- المبحث الأول: نقد القرصنة الروسية و الإستخبارات الأمريكية

- المبحث الثاني: الردود الأمريكية على القرصنة الروسية

- المبحث الثالث: السيناريوهات المستقبلية للصراع السيبراني الأمريكي - الروسي .(تصاعد الصراع - إنخفاض الصراع)

خاتمـــــة

قائمة المراجع و المصـــادر

فهــــرس المحتويـــات

مقـــدمـــة

مقدمــــــــــة :

القرصنة الإلكترونية أو المعلوماتي هي عملية إختراق لأجهزة الحاسوب بطريقة إحترافية، لكنها لا تتوقف عند أجهزة الحاسوب وإنما تشمل كل ما هو مرتب بالشبكات الإلكترونية كالإتصالات و أجهزة الساتيلايت.

فعملية السطو هذه تتطور بسرعة فائقة بإستخدام تقنيات حديثة و معقدة، تتم هذه العملية بعدة طرق و لأسباب مختلفة، أهمها الجوسسة، بدأت هذه الظاهرة التي تشمل الهجوم هي شبكات الحاسوب من قبل محترفي الأنظمة الإلكترونية، ففي عام 1986 م و ذلك من قبل شخص يدعى روبيرتو سوتو (Roberto Soto) ذو الجنسية الكولومبية، و الذي قام بسرقة خط تيليكس الحكومي ليرسل مجموعة رسائل عبره إلى مصارف في المملكة المتحدة، ومنها إلى دول أخرى، ونتج عن هذه الرسائل نقل 13.5 مليون دولار من أرصدة الحكومة الكولومبية، في عام 1988 زرع برنامج "Worm" في شبكة حواسيب حكومية و إنتشر في 6000 حاسوب وكشفت بعدها منظمة الحماية ضد السايبر أتاك، الطالب طالب جامعة كورل فطرد من الجامعة و حكم عليه إيقاف العمل لمدة 03 سنوات بالإضافة إلى دفع غرامة مالية بمبلغ 10.000 دولار، تزايد عدد القراصنة في القرن العشرين (20 م) ولم يقف الحد عند عتبة الوطن، فقد أصبحت حربا جديدة بين الدول و خاصة لما إتخذتها روسيا، ففي عام 1994، قامت مجموعة من القراصنة الروسية بنقل مبلغ 10 ملايين دولار من Bank وإلى حسابات مصرفية في مختلف دول العالم، و كان المشرف على هذه العملية فلاديمير كيفين الذي إستخدم حاسوبه الشخصي لتحويل الأموال إلى حسابات في فنلندا و إسرائيل، و قد تم إيقافه في الولايات المتحدة، و حكم عليه بالسجن لمدة ثلاث سنوات.

خلال عام 1995 تعرضت حواسيب وزارة الدفاع الأمريكية إلى 250.000 هجمة، كما تعرضت المواقع الفدرالية للتشويه، ولكن في عام 2001 م بلغت القرصنة الإلكترونية دروتها، فقد قام مجموعة من القراصنة المحترفين بإختراق الموقع الإلكتروني الأكثر حماية: موقع شركو مايكروسوفت للبرمجيات تم حل المشكلة خلال ساعات، ولكن هذه العملية ألحقت أضرار بالمواقع إذ أن الملايين لم يتمكنوا من تصفح الموقع لمدة يومين.

قراصنة المعلومات يصنفون إلى مجموعتين : " الهواة " أو مايسمونهم الهاكرز (Hackers)،و المحترفين الكراكز (Crackers)، الهواة (Hackers) يعتمدون على برامج التجسس الجاهزة و المتاحة في كل مكان، أي عن طريق الشراء أو التحميل من شبكة الأنترنت و مهام الهاكرز هو زرع ملفات التجسس من نوع Patches و Torjan في حواسيب الضحايا عن طريق البريد الإلكتروني أو ثغرات الويندوز التي يكشفها

البرنامج، الهدف من هذا النوع طفولي، لأن هؤلاء الهواة يسومن فقط لإثبات نجاحه، فما يشغلهم هو التسلل إلى الحواسيب، سرقة البريد الإلكتروني و التلاعب في الإعدادات و لكن يسهل إيجادهم إذ يتركون بصمة تدل على عبورهم.

أما الكراكز (Crackers) فهم محترفين و الأخطر فئة، لأنهم لا يخترقون الأجهزة دون سبب فعاليا ما يكون تحت تصرف الحكومة أو يعملون تحت وسائل الاستخبارات، يستخدمون أنظمة متطورة و يعتمدون غلى الألغوريتمية و لغات البرمجة و التشغيل.

أهدافهم مختلفة و خطيرة مثل سحب الأموال من حساب العمال أو الولوج إلى المواقع الحكومية لسرقة أسرار دولة ما، و ذلك بالتلاعب ببياناتها أو تدميرها، و يصعب تقفي أثرهم.

و من أهم القراصنة المحترفين أو الكراكز، فلاديمير لفين (Valdemir Levin) ، كيفين دايفيد ميتنيك (Kevin David Mitnick) و يوهان هيليسينجيوس (Johan Helsingius) .

كيفين ميتنيك إشتهر بإسم " Condor " على الشبكة المعلوماتية تم الحكم عليه أول مرة بالسجن لمدة سنة في إصلاحية، و اعتبر أول قرصان يكتب إسمه في أرشيف الأفا بي أي(FBI) بين المجرمين الأكثر طلبا، لاحقا عند خروجه من السجن نشر كتابا يتحدث عن عمليات الهاك أو القرصنة التي قام بها تحت إسم السبع في أسلاك التوصيل (Ghost in the Wires) مع ويليام سيمون(Wiliam L.Simon) .

بالإضافة إلى كيفن ميتنيك و الذي يعتبر من أهم القراصنة في القرن العشرين، نجد مجموعة 4/4

(The 4/4) و الذين أطلقوا هجومات على أنظمة أجهزة الحاسوب الرفيعة المستوى أو ما يسمى بـ

" High Profile Computer Systons "، من بينهم المختبر الوطني (Les Alms National) المختبر الوطني لوس ألموس، و سلون كاترينغ الذي هو مركز للحماية بمرضى السرطان و أيضا Security Pacific Bank و ذلك خلال 1982 و 1983 .

بينعام 1980 و 2000 قامت مجموعة أخرى تطلق على نفسها Legion Of Doom و على رأسها لوكس لوثر " Lex Luthor" بإختراق أهم المواقع الحكومية و ذلك بمساعدة كيفين ميتنيك (2012)

و الذي عرف بإحترافية لإيجاد عيوب في الأنظمة (syston Plans) ، وبفصل هذه العيوب، التي مهما بلغت جودة الحماية ضد القرصنة المعلوماتية، لا يمكن تفاديها.

تتم أغلب عمليات الإختراق عن طريق زرع برامج معينة في الأجهزة الإلكترونية، من بينها الفيروسات (Virus) ، هذه البرامج تملك القدرة على نسخ نفسها أكثر من مرة، وتتموقع في القرص الصلب (HArd Disk)، يمتاز بالتخفي و من أثاره تدمير أنظمة تشغيل الحاسوب، ميزة النسخ هذه تجعله يحل محل لملفات الأصلية.

أحصنة طروادة(Trojans) وهذه برامج التجسس، تجعل القراصنة في قدرة على الحصول على مبتغاهم وذلك ببرمجة على عمل معيين، مثل تحميل الملفات المهمة إلى حواسيب القراصنة.

و هناك أيضا الديدان (Worms)، وأشهرها Morris Worm أو Source Code الذي أطلقه روبرت تبان (Robert Toppen) ، والذي تحدثنا عنه سابقا، أطلق في نوفمبر 02 عام 1988، من جامعة Cornell و كان أول من سجن طرف CFAA 7، برنامج Worm يقوم بالهجوم على العيوب المعلوماتية و ذلك باستعمال Source Code، و عند إستقراره، ينتقل من جهاز لأخره

هناك أيضا القنابل المعلوماتية (Information Bombs) و الفخ (Trops) والتي كانت تستعملها مجموعة (Mastions of Deception) أو (Mod) بجانب مجموعات أخرة مثل Scorpion, Hac.

إنتقلت العدوى القرصنة من المجموعات المحلية إلى المنظمات الحكومية و ذلك بصدد الجوسسة رغم تصنيفها في مجال الجرائم السيبرانية لأن أضرارها أكثر من مبرزاتها، خوفا من الإرهاب المعلوماتي.

في أنثلوجية Cyber Space And National Security ديريك ريقيرون Darek S.Reverson (2012) قام بجمع مقالات حول القرصنة المعلوماتية، حيث نجد نيكولاس جفوسداف (Nikolons K.Gvosdev) يتحدث عن قدورات روسيا في هذه الحرب السيبرانية الحدبثة.

في عام 2009، الرئيس الروسي ديمتري ميدغيدف Dimitri Medvedv صرح أن روسيا كانت " بشكل ملحوظ متخلفة عن البلدان الأخرى في تطوير التقنيات المتقدمة خاصة في مجال أجهزة الكمبيوتر

" Russia Was Signiconth Behind Other Contines in developing العملاقة advanced Technolgies, path whorly in the filed of super computers "

في مجال الحرب الإلكترونية، أُبتت روسيا أنها رائدة و ذلك لأنها لم تمتنع عن وضع " هاك أكتفيست"

" Hack h visit " روسيين و أثبتوا مهاراتهم في الهجوم و تعطيل البنية التحتية " Infrastcuture " للكمبيوتر و للإتصالات الخاصة بإستونيا (Estonia) في 2007، و تعتبر هذه الهجومات من أول الحروب المعلوماتية في العالم، ولكن في 2008، صدرت روسيا هجوماتها السيبرانية ضد جورجيا (Georgia)، وكانت هذه أكثر أهمية أهمية، لأن هذه المرة وقعت في تنسيق واضح مع العملية العسكرية المستمرة و التقليدية، و قد بلغت المؤسسات العسكرية و الحكومية الغربية تقارير عن إجراء تحقيقات إلكترونية منتظمة من مصادر روسية حيث وقع هجوم خطير ضد وزارة الدفاع الأمريكية و في أواخر 2008.

في سبتمبر 2010 في أورينبورغ (Oreburg)، صرح الرئيس الروسي قائلا " الكمبيوتر الأن ليس أقل هو في الواقع أكثر أهمية، لأن جميع العمليات الحكومية تقريبا، بما في ذلك السيطرة على القوات المسلحة، و يحدث الأن بمساعدة أجهزة الكمبيوتر.

القرصنة المعلوماتية اليوم تزعزع إستقرار الدول و نقلب أنظمة الحكم فيها، وهكذا لم تعد الإنترنت سلاحا فحسب، بل أصبحت كذلك جيشا و جرائمها إرهابا (Don Verton 200)، في الدورة الثانية و السبعين للجمعية العامة للأمم المتحدة عقدت إجتماعا حول حماية مبدأ سيادة الدول – أحد أهم ركائز المنظمة الأممية – فجرائم الأنترنت تتصاعد خطورتها و صنفت في جرائم الحرب الإلكترونية، مما أدى رئيسة وزراء بريطانيا إلى دعوة لمؤتمر دولي يهدف إلى منع إنتشار التطرف و الإستخدام الإرهابي للأنترنت .

في 2016، أفاد تقرير للبيت الأبيض بأن القرصنة الإلكترونية كلفت الولايات المتحدة بين 57 و 109 مليار دولار .

إستخدام الهجمات السيبرانية بدل على حدوث تحول في تفكير ونهج مؤسسة الأمن القومي في الكرملين (Kremlin) خلال العقود الثلاثة الماضية، من الحقبة السوفياتية المعتمدة على النفوق العسكري التقليدي الساحق كعامل أساسي للتأثير على " توازن القوى " على الساحة العالمية إلى تقدير أكبر الأدوات غير العسكرية للقوة الوطنية – لتحقيق الأهداف الروسية " إن لم يكن من خلال الدبابات، إذن من قبل البنوك، بالإضافة إلى

زيادة التقدير لكيفية السيطرة على إمدادات الطاقة و كذلك إستخدام القوى الإقتصادية و المالية الأخرى كأدوات للقوة الوطنية، هناك تقدير متزايد لما يمكن تحقيقه في الفضاء السيبراني (Cyber Space) موضوع تطرأ له مباشرة الرئيس الروسي ميدفيدف (Medvedev) .

مند دخول العالم في الفضاء السيبراني، وحتمية إستخدام الأنترنت في تزايد، أصبحت السيطرة على الجول و تسريب المعلومات سهلة الإقتناء، وذلك ما زاد من مخاوف الحروب السيبرانية و الإرهاب السيبراني الذي لا يشمل فقط إقتناء المعلومات السرية لأنظمة الحكومية، و إنما إختراق الأنظمة الحاسوباتية في كل المجالات بما فيها الإقتصادية و المالية و الطاقوية، إذ أنه في وقتنا الحالي كل شيء يتم تسييره إلكترونيا، أي يتطلب تواجد الأنترنت، و لذلك في بحثي هذا أترضأ على دراسة الهجومات السيبرانية (Cyber Attack) مع التركيز على هجومات روسيا على أمريكا في الأونة الأخيرة و الوقوف عند مبدأ حتمية التخابر و التجريم الدولي.

في الفصل الأول سيتم النظر إلى ماهية الرصنة و طرق معنها، و كذلك دور القانون الدولي في التجريم القرصنة و الحروب السيبرانية بالإضافة إلى ظاهرة ويكي ليكس (Wikilix) و الفرنسية الروسية للانتخابات الأمريكية الأخيرة، أما في الفصل الثاني فالتركيز يكون على الصراع الدولي الأمريكي و سلاح الأنترنت، و الفصل الأخير يتمركز حول مشكلات و عيوب القرصنة و علاقتها بالعمل الإستخباراتي .

وبناء على ما تقدم بالإمكان طرح الإشكالية التالية للاقتراب من تفسير الظاهرة المبحوثة على النحو التالي:

هل يمهد هذا التهديد الروسي للأمن القومي لدول الاخرى الى حرب ايديولوجية اخرى و ماذا سوف ينتج من هذه الحروب السيبرانية ؟

ودعما لهذه ألإشكالية بالإمكان طرح التساؤلات التالية للاقتراب أكثر من فهم وتفكيك الظاهرة المبحوثة على النحو التالي:

1- **هل هنالك قانون روسي يحمي الهاكرز من تهديدها لأمن القومي ؟**

2- **ما هو موقف الامم المتحدة من القرصنة السيبرانية ؟**

3- **هل هنالك تعاون روسي وصيني في اختراقات المواقع الحكومية و تهديد امن القومي لدول ؟**

4- **هل كان هنالك تعاون روسي امريكي في توقيف هاته الاختراقات ؟**

5- هل هناك حرب ايديولوجية اخرى في طريق النشأة ؟ وماذا سينتج من هذه الحروب السيبرانية ؟

6- ماهي عواقب استخدام القرصنة الالكترونية من طرف الدول المتقدمة على الدول النامية ؟

7- كيف يتم حماية الدول من هذه الحروب الجديدة ؟ و ما هي الإجراءات اللزمة التي يمكن اتخاذها ؟

8- هل كان هنالك تخابر من اجل القبض على القراصنة ؟

ستعتمد الدراسة على الفرضيات التالية:

الفرضية الأولى: كلما احتجت الحكومات لدعم الأنتلجنسيا المخابراتية تحولت السياسات إلى حرب للمعلومات

الفرضية الثانية: كلما استخدمت موسكو المخابرات اضطرت الإدارة الأمريكية للرد.

الفرضية الثالثة: كلما استخدمت واشنطن العمل الإستخباري اضطرت إلى إقناع الكونغرس الأمريكي بحتمية التخابر.

الفرضية الرابعة: كلما قلت الرقابة التشريعية و القضائية على المخابرات أدى ذلك إلى تهديد إستقرار الدول.

- الأهمية العلمية و العملية للموضوع:

- الأهمية العلمية للموضوع:

- هذا الموضوع الذي نتطرق اليه سيكون بهدف تبين خطر القرصنة الإلكترونية على أمن و إستقرار الدول وهو مايدل على حتمية البحث في هذا المجال بالجزائر .

- دراسة دوافع روسيا للإختراق مواقع الحكومة الأمريكية بين حتمية الجوسسة و الإجرام الدولي لفهم التحولات الدولية.
- التعرف على هذه الظاهرة على الصعيد الماكرو-السياسي (**Macro-politics**) و الميكرو-السياسي و أثرها على إستقرار الدول (**Micro-politics**)
- توضيح كيفية الحماية من القرصنة و إستخدام تشريعات الحماية الوقائية .
- الإستدلال و الإطلاع بمناهج الدول المتقدمة لحماية نفسها من القرصنة المهددة .

- الأهمية العملية للموضوع:

ـ التمرّن على منهجية البحث العلميّ، وتقنيات كتابة البحوث، وكيفية البحث في مجال تقني يخص حرب المعلومات.

ـ تحليل مضمون الوثائق العسكرية للجزائر وحلف الناتو وتعلم كيفيات دراسة المحتوى القانوني للمعاهدات الدولية.

ـ استخدام البحث الجغرافي الجيوبوليتكي لدراسة الأبعاد الجيوبوليتيكية للظاهرة المبحوثة و انعكاساتها الإقليمية.

أسباب اختيار الموضوع:

الأسباب الذاتية:

- التدريب على البحوث التقنية و التعرف على الدراسات الخاصة بالتهديدات الغير التقليدية .
- الرغبة في تحضير هذا البحث العميق الشاسع و الإنخراط في النقاش العالمي حول التحولات الأمنية.

الأسباب الموضوعية:

- نظرا لأهمية هذا الموضوع الذي لم يطرح بعد بشكل عميق بالجامعات الجزائرية.
- نظرا للقوة الروسية في حتمية التخابر و حتمية الإطلاع على الدراسات المتخصصة حول هذا المجال.

الإطار النظري: ستعتمد هذه الدراسة على عدة نظريات

1- نظرية "الفوضى" لألكسندر فاندت

تشترك نظرية النزاعات الدولية ونظرية الفوضى في العلاقات الدولية في الجذر الأساسي لكليهما، حيث تقتربان من مقاربات النظرية الواقعية في العلاقات الدولية: (النزعة الشريرة للطبيعة البشرية، القوة والمصلحة أساس العلاقات الدولية، مقاربة توماس هوبز حول القوة ونيكولاس ميكيافيلي في الاستبداد، النزعة البراجماتية الذرائعية، الفوضى والتنافس الدوليّ.

2- نظرية "صناعة القرار" و "نظرية الدور"

و"نظرية السياسة الخارجية"..

تتأسس السياسة الخارجية على مفاهيم الفعل وردّ الفعل، كمنطلق لتخطيط دور الدولة في المسرح الدوليّ، والمشاركة في إدارة العلاقات الدولية، وأنشطة السياسة الدولية، من خلال قرارات الساسة والدبلوماسيين المسؤولين عن صنّاع القرار، وتتأسّس السياسة الخارجية على فكرة تحويل المعلومات إلى رسائل سياسية تخدم مصالح الدولة، عبر صوغ سياسات متوقعة لأدوار منتظرة للدول.

3- نظرية الحرب "اللامتماثلة/اللاتناظرية"

(الحرب على الإرهاب) والتدخل الدولي الإنساني (مبدأ التفويض)

فرض تحدّي **الحرب العالمية على الإرهاب،** تعاونا دوليا جديدا في عصر العولمة، الذي أتاح تواصلا ايجابيا بين مختلف الفواعل عبر العالم، دون أن يتحكم في الجوانب السلبية لظاهرة "عولمة التهديدات الأمنية" ، لذلك يصطلح بعض المفكرين على اعتبار الحرب على الإرهاب "حرب معلومات" بالأساس لما يمكن الاصطلاح على تسميته "الجريمة السياسية المنظمة.

4- نظرية الحرب الوقائية (الجيل الرابع)

فالكلمة كما ذكرت في اللغة الذي يقصد به منع Praevenire صفة مشتقة أساسا من الفعل اللاتيني Preventive الإنجليزية شيء ما من الحدوث، كما ورد في قاموس أكسفورد الإنجليزي:

To prevent: “to forestall, to deprive of power, or hope of acting or succeeding”.

يرى المفكر العربي إسماعيل صبري، أن الحرب الوقائية تعتبر المظهر الرئيسي لتخطيط الإستراتيجية النووية على الأساس الهجومي البحت، حيث يسعى طرف معين إلى احتضان هذه الإستراتيجية التي تضمن إلحاق أكبر قدر ممكن من الدمار بالخصم، ويعتبر ذلك بمثابة البديل الأفضل للإستراتيجية الدفاعية، بصرف النظر عما يوضع تحت تصرف هذه الإستراتيجية من إمكانيات.

5- نظرية الأمن القومي:

كان قيام الدراسات المهتمة بالأمن القومي متوافقاً مع ظروف عالمية سياسية وعسكرية جديدة أعقبت الحرب العالمية الثانية والتوازنات والتكتلات والمحاور التي نتجت عن الحرب بين القوى الدولية، بالإضافة إلى الانتشار الكثيف للأسلحة والتطور النوعي الذي شهدته هذه الأخيرة، والذي أدى إلى تعديلات في النظام الدفاعي العالمي وثوابته التقليدية الموروثة، وفرض رؤية جديدة للأمن، وتحديداً جديداً للمجال الأمني للدول.

6- نظرية القانون الدولي:

تعددت تعريفات القانون الدولي العام، ويرجع هذا الاختلاف إلى التطور الذي عرفه هذا الفرع من القانون سواء من حيث الأشخاص أو الموضوعات التي يحكمها.و القانون الدولي العام هو مجموعة من القواعد القانونية التي تنظم العلاقة بين الدول او بين الدولة و الاشخاص باعتبارها شخصية ذات سيادة. و ينقسم القانون الدولي العام إلى قانون عام داخلي و قانون عام خارجي.

مناهج الدراسة:

تستخدم هذه الدراسة **المنهج التاريخي** لدراسة الأطوار السابقة والحالات السابقة للظاهرة، كما تستخدم **المنهج الوصفي والمنهج التحليلي** لتقديم المعلومات عن الظاهرة المبحوثة، و **المنهج القانوني** **ومنهج تحليل المضمون** للإطلاع على **الوثائق القانونية و التشريعية**.

مجالات الدراسة:

- **المجال الزماني**: من 2000 إلى 2018 (بعد الدخول إلى الموجة الثالثة)
- **المجال المكاني**: روسيا و (و.م.أ)
- **المجال الموضوع**: التجريم الدولي و حتمية التخابر للاستخبارات

صعوبات الدراسات:

تكمن الصعوبات في كثرة المقالات وقلة الدراسات خاصة الكتب الأكاديمية في المجال، مما يدفعني إلى الاستعانة بالدراسات الغربية المنشورة على صفحات الأنترنيت.

الـــفصـل الأول:

ماهيــة القرصنـــة و طــرق منعهـــا

الفصل الأول: ماهية القرصنة و طرق منعها

المبحث الأول: ماهية القرصنة و الحروب السيبرانية

ماهية القرصنة الإلكترونية:

يشهد العالم في الفترة الراهنة نوعا جديدا من سباق التسلح، لا على غرار المعروفة منها في حقل الأسلحة التقليدية و غير التقليدية، و يقوم هذا السباق على إستحداث أو تطوير برامج إلكترونية معدة لإغراض عسكرية تعرف إختصار بالسايبر Cyber

عندما يتبادر إلى أسْماعنا كلمةُ قرصنة، فإنَّنا نتخيَّل عصابات سرقة السُّفن البحريَّة والسَّطو عليها، ونَهْب ما فيها وأَسْر طاقمها، وهو ذاته ما يفعله قرصان الأنظمة الإلكترونيَّة بالضبط، لكن بوسائل حديثة، ودون أن يعرِّض نفْسَه للخطر.

فالقرصنة الإلكترونية أو المعلوماتيَّة هي عمليَّة اختراق لأجهزة الحاسوب تتمُّ عبْر شبكة الإنترنت غالبًا؛ لأنَّ أغلب حواسيب العالَم مرتبطة عبْر هذه الشَّبكة، أو حتَّى عَبْر شبكات داخليَّة يرتبط فيها أكثرُ من جهاز حاسوب، ويقوم بِهذه العمليَّة شخصٌ أو عدَّة أشخاص متمكِّنين في برامج الحاسوب وطرُقِ إدارتِها؛ أيْ: إنَّهم مُبَرْمِجون ذوو مستوًى عالٍ يستطيعون بواسطة برامج مساعدة اختراق حاسوب معيَّن والتعرُّفَ على محتوياته، ومن خلالها يتم اختراق باقي الأجهزة المرتبطة معها في نفس الشبكة.

تاريخ القرصنة:

بدأَتْ ظاهرة القرصنة والاختراق مع بداية ظهور الحاسبة الإلكترونيَّة، وازدادت بشكل كبير مع استخدام تقنية الشَّبكات؛ حيث يشمل الاختراقُ الهجومَ على شبكات الحاسوب من قِبَل مُخترقي الأنظمة الإلكترونيَّة ومنتَهِكي القوانين، كما يبيِّن التطوُّرُ الحاصل في مَجال سرِّيَّة المعلومات التي تغطِّي الإنترنت بالإضافة إلى تقنيات أخرى كالاتِّصالات [1].

إنَّ عمليات القرصنة تتطوَّر وبِسُرعة فائقة باستخدام تقنيات حديثة ومعقَّدة؛ مِمَّا جعل النَّظرة إليها تتغيَّر كليًّا عمَّا كانت عليه في المراحل السَّابقة، وسأُحاول سرْدَ أهمِّ حالات القرصنة الَّتي حدثت عبْر التاريخ، وهي كما يلي:

[1] أسامة سمير حسين،**الإحتيال الإلكتروني**، الأسباب و الحلول، الجنادرية للنشر و التوزيع، ط1، 2011

1- في عام 1986م قام شخصٌ يدعى (روبيرتو سوتو) كولومبِيٌّ الجنسيَّة (بسرقة خطِّ تيليكس حكومي؛ لِيُرسل مجموعة رسائل عبْرَه إلى مصارفَ في المملكة المتَّحِدة، ومنها إلى دول أخرى، ونتج عن هذه الرسائل نَقْل 13,5 مليون دولار من أرصدة الحكومة الكولومبيَّة.

2- في عام 1988 قام أحدُ طلاَّب جامعة كورل بزراعة برنامج Worm في شبكة حواسيب حكومية انتشر خلالَها في 6000 حاسوب، وبعد أن تم كشْفُه، طُرِد من الجامعة، وحُكِم عليه بإيقافه عن العمل 3 أعوام، وتغريمه مبلغ) 10,000عشرة آلاف دولار.

3- مجْموعة من القراصنة الرُّوس قاموا بنقل مبلغ 10 ملايين دولار من City Bank إلى حسابات مصرفيَّة في مُختلف دول العالم في عام 1994م، وكان زعيم العصابة "فلاديمير ليفين" يستخدم حاسوبه الشخصيَّ لتحويل الأموال إلى حسابات في كلٍّ من فنلندا وإسرائيل، وقد تمَّ إيقافه في الولايات المتحدة، وحُكِم عليه بالسجن لمدة ثلاث سنوات.

4- خلال عام 1995 تعرَّضَت حواسيبُ وزارة الدِّفاع الأمريكيَّة إلى 250,000 هجمة، كما تعرَّضَت المواقع الفيدرالية للتَّشويه.

5- قامت مجْموعة من القراصنة باختراق الموقع الإلكتروني لشركة مايكروسوفت للبرمجيَّات عام 2001م، وعلى الرغم من أن المشكلة تم حلُّها خلال ساعات قليلة، إلاَّ أن الملايين لم يتمكَّنوا من تصفُّح الموقع لمدَّة يومَيْن.

6- في عام 2007م قام قُرْصان تركي يدعى karem بالْهُجوم على موقع منظَّمة الأمم المتحدة على شبكة الإنترنت.

تصنيف قراصنة المعلومات:

1- الْهُواة (الهاكرز):Hackers

يعتمد الْهُواة على برامج التجسُّس الجاهزة والمتاحة في كلِّ مكان، سواء عن طريق الشِّراء أو التحميل من شبكة الإنترنت، ويقوم الهاكرز بزرع ملفات التجسُّس patches &Trojans في حواسيب الضَّحايا عن طريق البريد الإلكترونِيِّ أو ثغرات الويندوز التي يكتشفها البرنامج، هذا الصِّنف من الهاكرز أهدافه طفوليَّة؛ حيث يسعى لإثبات نَجاحه في استخدام هذه البرامج وانضمامه إلى قائمة الهاكرز؛ بِهَدف التفاخر بين الأصحاب كشخصٍ يَمتلك مواهِبَ يفتقدها بعضُهم، وهؤلاء كلُّ ما يشغلهم هو التسلُّل إلى حواسيب الآخرين وسرقة بريدِهم الإلكتروني، والتلاعب في إعدادات هذه الأجهزة، مع تَرْك ما يفيد أنهم فعلوا ذلك كشكل من أشكال الغرور والتباهي بالنَّفْس[1].

[1] http://coeia.edu.sa/index.php/ar/assurance-awamess/articles/51-forensic-and-computer-crimes/2012/22
تاريخ الدخول: 22/04/ 2018

2- المحترفون (الكراكرز) Crackers :

أمَّا المحترفون فهم الفريق الأخطر؛ لأنَّهم يعلمون ماذا يُريدون، وماذا يفعلون، وكيفية الوصول إلى أهدافهم باستخدام ما لَدَيْهم من علم يطوِّرونه باستمرار، بالإضافة إلى استخدام البَرامج الجاهزة المتطوِّرة، إلا أنَّهم يعتمدون على خبرتِهم في لغات البَرمجة والتشغيل، وتصميم وتَحْليل وتشغيل البَرامج بسرعة، كما أنَّ هوايتهم الأساسيَّة معرفة كيفيَّة عمل البرامج لا تشغيلها[1].

إنَّ أهداف هذا الفريق أكبَرُ وأخطر من الفريق السَّابق؛ فأهدافُهم المصارف وسَحْب الأموال من حساب العُمَلاء، أو الولوج إلى أخطر المواقع وأكثرها حساسيَّة، والتلاعب ببياناتها أو تدميرها.

مهارات الهكرز:

للهكر مهاراتٌ، وهي أنَّهم يستطيعون اختراق مواقع الشركات، واختراقَ وفكَّ كلمة السرِّ، سواء الخاصَّة بالبريد الإلكتروني، أو موقع شركة على الإنترنت، أو فكِّ "السيريال نَمْبر" عند تثبيت برنامج[2].

أشكال القرصنة:

1- القرصنة الهاتفية:

المقصود بالقرصَنة الْهاتفيَّة هنا هو إجراء مكالَمات هاتفيَّة دون تسديد أجرة المكالمة، ويتمُّ ذلك باستعمال)علب إلكترونية (تَحُول دون عمل معدَّات احتساب المكالمة.

2- قرصنة البرامج المحلية:

هذه القرصنة هي كناية عن تَجاوز البرمَجيَّات التي توضع للحَوْل دون اختلاس نُسَخ البرامج الحاسوبيَّة التطبيقية؛ أيْ: بصورة غير مأذونة.

ولقد بدأ ازدهار هذا النَّوع من القرصنة في الثمانينيَّات في بلغاريا، حيث كان القراصنة يقومون بنَسْخ البرامج الحاسوبيَّة الغربيَّة لإعادة تصديرها إلى سائر بلدان أوربا الشرقية، وكثيرًا ما يقوم هؤلاء القراصنة أنفسُهم بتطوير فيروسات حاسوبيَّة جديدة أيضًا.

---

[1] david I Cave & William Vastrroch: **Computer Crime Acrime Fight** (Reilly&Associte, nc1995) P 61.

[2] عمر محمد أبو بكر بن يونس: "**الجرائم الناشئة عن استخدام الانترنت الجوانب الموضوعية و الإجرائية**"، (القاهرة: دار النهضة العربية، 2004) ص 141،140.

ومعظم القراصنة من هذه الفئة في البلدان الغرْبية هم إمَّا تلاميذ ثانوية مولَعُون بألعاب الفيديو، أو طلاَّب جامعيُّون، والصفة الغالبة أنَّهم من المولعين بالكمبيوتر والتكنولوجيا الإلكترونية، ويؤْمِنون بوجوب مجَّانية استعمال الشبكات الحاسوبيَّة على أساس أنَّ ذلك يسهِّل عملية اتصال الناس، ويوثق العلاقات الاجتماعية، والصداقة بين الأُمَم والشعوب.

الأسباب التي تدفع إلى ارتكاب جرائم القرصنة المعلوماتيَّة:

يختلف مرتكبو جرائم القرْصَنة المعلوماتيَّة عن مرتكبِي الجرائم الاعتياديَّة من حيث المبدأُ وطريقةُ القيامِ بالعمل الإجراميِّ، لكن في النهاية يبقى الطَّرَفان مُخالفَيْن للقانون؛ لذا يستحقَّان العقابَ بِما اقترفوا من جرائم[1].

وهناك عدَّة أسباب تدفع إلى ارتكاب الجرائم المعلوماتيَّة، يُمكن أن أختصرها بالآتي:

1-حب التعلم:

يعتبر حبُّ التعلم والاستطلاع من الأسباب الرئيسة التي تَدْفع إلى ارتكاب مثل هذه الجرائم؛ لأنَّ الْمُخترِق يعتقد أنَّ أجهزة الحاسوب والأنظمة هي ملك للجميع، ويجب ألاَّ تبقى المعلومات حكرًا على أحد؛ أيْ: إنَّ للجميع الحقَّ في التعرُّف والاستفادة من هذه المعلومات[2].

2- المنفعة المادية:

قد تكون مُحاولات الكسب السريع، وجَنْي الأرباح الطائلة دون تعَب، ولا رأس مال، من الأسباب التي تَدْفع إلى اختراق أنظمة إلكترونيَّة كالتي تستخدمها الْمَصارف عن طريق الدُّخول إلى الحسابات المصرفيَّة، والتلاعب فيها، أو الاستخدام غَيْر المشروع لبطاقات الائْتِمان.

3- التسلية واللهو:

عددٌ غير قليل من مُخترقي الأنظمة يتَّخِذون مِن عمَلِهم هذا وسيلة للمرح والتَّسلية، وتقضية أكبر وقت مُمْكن في أنظمة وحواسيب الآخرين، ويكون هذا الاختراق غالبًا سِلْميًّا، ودون أن يَحْدث تأثير يُذْكر[3].

---

[1] محمد على العريان:" **الجرائم المعلوماتية**"، ط1 (الأسكندرية: دار الجامعة الجديدة، 2004) ص 66.
[2] انتصار أنور الغريب: " **أمن الكمبيوتر و القانون**"، (بيروت: دار الراتب الجامعي، 1994) ص 10 .
[3] رمسيس بهنام:" **المجرم تكوينا و عقيدة**"،(الأسكندرية: منشأة دار المعارف، ب ت) ص 175

4- الدَّوافع الشخصية:

يعتبر مُحيط الإنسان والبيئة التي يعيش فيها من العوامل المؤثِّرة في سلوكه وتصرُّفاته، وغالبًا ما تدفع مشاكل العمل إلى رغبةٍ في الانتقام ووجود أنظمة إلكترونيَّة تسهِّل له القيام برغباته، فيَعْبث بمُحتوياتِها إلى درجة التَّخريب، أو يكون الدافع التحدِّي وإثبات الجدارة أمام الآخرين بِحَيث يفتخر هذا الشخص بأنَّ في استطاعته اختراقَ أيِّ حاسوب أو أيِّ نظام، ولا يستطيع أحدٌ الوقوف في وجهه[1].

كيف يتمكن الهاكرز من الدخول إلى جهازك ؟

عندما يتعرَّض جهاز الكمبيوتر للإصابة بِملفِّ التجسُّس وهو (الباتش أو التروجان)، فإنَّه على الفور يقوم بفَتْح بورت (port) أو منفذ داخل جهازك، فيستطيع كلُّ من لدَيْه برنامج تَجسُّس أن يقتحم جهازك من خلال هذا الملفِّ الذي يقوم بفتح منطقة أشبه بالنافذة السرِّية التي يدخل منها اللُّصوص، وهم الهاكرز!

قراصنة مشهورون:

1- فلاديمير ليفين: Vladimir Levin "

ذكيٌّ في الرياضيات، وهذا أحدُ أهمِّ أسباب اعتقاده بشهرته, تَخرَّجَ مِنْ جامعةِ "بيترسبيرغ تيخنولوجيتشيسكاي"، وكَانَ العقل المدبِّر وراء عصابة لصِّ الكومبيوتر الرُّوسيةِ، التي استدرجَتْ حاسباتِ "سيتيبانك" إلى إعْطاء الـ10$ مليون.

2- " يوهان هيلسينجيوس: Johan Helsingius "

معروف بإنشاء باعث رسائل البريد الإلكتروني، المشهور، والْمُسمَّى ب"بنت.في.(**Penet**.**fi**)"

3- كيفين ديفيد ميتنيك: Kevin Mitnick "

اسم الشهرة له على الشبكة كان" كوندور.**Condor** "، كمُراهق لَمْ يستطع أن يوفِّر لنفسه حاسوبه الخاصَّ, وإنَّ إحدى الأشياء غير العادية عن "ميتنيك" أنه استعمل غُرَف المحادَثة في الإنترنت لإرسال رسائل لأصدقائه, وقد تَمَّ الحكم عليه أوَّلَ مرَّة بالسجن لِمُدَّة سنة في إصلاحيَّة، و"كيفن" من القراصنة الخالدين؛ حيث اعتُبِر أوَّل قرصان يُكتب اسْمُه في لوائح الإف بي أي بيْن المجرمين الأكثر طلبًا.

[1] محمد عبد الله المنشاوي: **جرائم الانترنت من منظور شرعي و قانوني**، بحث منشور على الانترنت (مصدر) تاريخ الدخول 2018/03/20 www.minshawi.com

أهمُّ طرق اختراق الحاسوب:

تتمُّ أغلب عمليات الاختراق عن طريق زَرْع برنامج معيَّن في جهاز الضحيَّة، يقوم هذا البرنامج بعمل معيَّن، كما يلي:

1- الفيروسات :Virus

هو برنامج له القدرة على نَسْخ نفسه أكثر من مرَّة، ويَمتاز بقدرته على التخفِّي، وله آثار تدميريَّة على أنظمة تشغيل الحاسوب؛ لأنَّ عملية النَّسْخ والتَّكرار الدائم لِملفَّاته تَجْعل هذه الملفات تحلُّ محَلَّ الملفات الأصلية الموجودة على القرص الصلب **Hard Disk** للحاسوب[1].

2- أحصنة طروادة :Trojans

وهو برنامج تجسُّسي، يقوم بعمل معيَّن يحدِّده الشَّخصُ الذي صمَّمَه أو زرَعَه في جهاز الضحية، يُمكِّنه من الحصول على مبتغاه.

3- الديدان :Worms

هو برنامج ينتقل غالبًا عبْر البريد الإلكتروني، ويَمتاز بقدرته على التنقُّل عبْر شبكات الإنترنت؛ لغرَضِ تعطيلها أو التشويش عليها عن طريق شلِّ قدرتها على تبادل المعلومات.

4- القنبلة المعلوماتية :Information Bomp

هو برنامج يصنعه مصمِّمُ النِّظام نفسه؛ لغرض إنْهاء مدَّة عمل ذلك النظام خلال وقتٍ معيَّن، أو في حال استخدام أرقامٍ أو أحرف معيَّنة يُحدِّدها المصمِّم.

5- الفخ :Trappe

هو مُنفذ يتركه مصمِّم البرنامج يسهِّل له عملية الدُّخول إليه وقت ما يشاء، وإجراء التعديلات التي يُريدها.

[1] عبد الله علي عبد الله، **تقنيات الاختراق المادي**، دار البشائر الإسلامية-بيروت،ط1، 2003،ص 78 – 89

الحرب السيبرانية :

في ظل تحول الفضاء الالكتروني كمجال جديد للتفاعلات الدولية برزت حالة توظيفه في الاستخدامات المدنية والاخرى ذات الطبيعة العسكرية ،وأضحى مثل غيره من المجالات الدولية كالبر والبحر والجو،وتبلورت الانشطة العدائية العنيفة في ظاهرة الحروب السيبرانية التي اتسمت بتعدد مظاهرها وخصائصها والفاعلين فيها،والتي ظهرت عبر نمطين اساسين نمط يتعلق بتوظيف القوة الناعمة في الصراع عبر الفضاء الالكتروني، والنمط الاخر يتعلق بتوظيف القوة الصلبة في الصراع عبر الفضاء الالكتروني وهو ما يعكس تنامي في القدرات والتهديدات وتعاظم التاثير على أمن البنية التحتية الكونية للمعلومات[1].

يطلق على الحرب الإلكترونية "الحرب السيبيرية" لأنها شبيهه بالحرب, حيث يهاجم القراصنة "Hackers" الملفات والمواقع وغيرها التي تخص الاخرين وبذات الوقت يدافع الناس عن معلوماتهم من القراصنة عن طريق برامج وطرق متعددة.

أما كلمة "سيبيرية" أو "سايبورغ" فهي كلمة بدأ استخدامها عام 1960 والتي اطلقها مانفريد كلاينس وناثان كلاين في مقال لهما ويعني المصطلح: المزج بين الاليكترونيات والأنسان.

وتعبير "الحرب السيبرانية" يُستخدم من قبل فئات عديدة من الناس للإشارة إلى أشياء مختلفة. ويُستخدَم المصطلح هنا للإشارة إلى وسائل وأساليب القتال التي تتألف من عمليات في الفضاء الإلكتروني ترقى إلى مستوى النزاع المسلح أو تُجرى في سياقه، ضمن المعني المقصود في القانون الدولي الإنساني. ويساور اللجنة الدولية قلق بشأن الحرب السيبرانية بسبب ضعف الشبكات الالكترونية والتكلفة الإنسانية المحتملة من جراء الهجمات السيبرانية. فعندما تتعرض الحواسيب أو الشبكات التابعة لدولة ما لهجوم أو اختراق أو إعاقة، قد يجعل هذا الأمر المدنيين عرضة لخطر الحرمان من الاحتياجات الأساسية مثل مياه الشرب والرعاية الطبية والكهرباء.[2]

وإذا تعطلت أنظمة تحديد المواقع GPS عن العمل، قد تحدث إصابات في صفوف المدنيين من خلال تعطيل عمليات إقلاع مروحيات الإنقاذ على سبيل المثال. ويمكن أن تتعرض السدود والمحطات النووية وأنظمة التحكم في الطائرات لهجمات سيبرانية نظرًا لاعتمادها على الحواسيب. وتكون الشبكات مترابطة إلى حد يجعل من الصعب الحد من آثار هجوم سيبراني ضد جزء من المنظومة دون الإضرار بأجزاء أخرى أو تعطيل المنظومة بأكملها. وقد يتضرر صالح مئات الآلاف من الناس، وصحتهم وحتى حياتهم. وتذكر اللجنة الدولية جميع أطراف النزاع بتوخي الحرص بشكل مستمر من أجل حقن دماء المدنيين، وهو أحد أهم الأدوار التي تقوم بها، فالحروب لها قواعد وحدود تنطبق على اللجوء إلى الحرب السيبرانية بنفس القدر الذي تنطبق به على استخدام البنادق والمدفعية والصواريخ.

---

[1] ايهاب خليفة، **القوة الالكترونية...كيف يمكن ان تدير الدول شؤونها في عصر الانترنت**، القاهرة: العربي للنشر و التوزيع،ط1، 2017.

[2] عادل عبد الصادق، **الارهاب الالكتروني: القوة في العلاقات الدولية: نمط جديد و تحديات محتلفة**، (القاهرة، مركز الأهرام للدراسات السياسية و الإستراتيجية، 2009) ص 30،40

اولا :هجمات الفضاء الالكتروني بين توصيف "الارهاب "او "الحرب".

من ضمن التعريفات لـ" "الحرب الإلكترونية" Cyber war بأنها تشير إلى التطبيقات العسكرية للفضاء الإلكتروني،وتنسيق الهجوم الإلكتروني والذي يتم شنه من قبل الدولة أو الفاعليين من غير الدول في إطار متبادل أو من طرف واحد، عبر ساحة الفضاء الالكتروني.

وعلي الرغم من الاستخدام الواسع في وسائل الإعلام لمسمي "الحرب الإلكترونية "، وهو مصطلح قديم كان مقصورا على رصد حالات التشويش علي أنظمة الاتصال والرادار وأجهزة الإنذار، بينما يكشف الواقع الحالي عن دخول شبكات الاتصال والمعلومات إلي بنية ومجال الاستخدامات الحربية.

و"يتم توصيف الاعمال العدائية عبر الفضاء الالكتروني والتي تستهدف تهديد البنية التحتية للمعلومات لتحقيق عدة اغراض ذات طبيعة سياسية واقتصادية واجرامية ، وهو ما ينعكس على عملية توصيفها وبخاصة مع امكانية التداخل الوظيفي بين عدة اهداف بشكل يصعب معة تحديد المسمى الصحيح لها، وهو ما يضيف ابعاد جديدة للمفهوم ، ومن ثم هناك من يفضل ان يستخدم تعبير "الحروب السيبرانية" تعبيرا عن حالة التوجه الجديد،ولكن تبقي كلمة "الحرب" هي الاخرى محل جدل وبخاصة ان هناك العديد من المسميات التي تطلق على تلك الانشطة العدائية عبر الفضاء الالكتروني . وهو ما يدفع الى اعادة النظر في اطلاق مسمى "الحرب" على تلك الانشطة العدائية ،وذلك يرجع الى ان مفهوم الحرب "تقليديا" يرتكز بالأساس علي استخدام الجيوش النظامية،وكان يسبقها إعلان واضح لحالة الحرب وميدان قتال محدد.أما في هجمات الفضاء الإلكتروني، فإنها غير محددة المجال أو الأهداف،كونها تتحرك عبر شبكات المعلومات والاتصال المتعدية للحدود الدولية أو اعتمادها علي أسلحة إلكترونية جديدة تلائم السياق التكنولوجي لعصر المعلومات،والتي يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق العملاء لأجهزة الاستخبارات.[1]

ومن ثم فانها ان لم يتم توصيف تلك الاعمال العدائية "بالحرب"، فان وصف عملية استخدام هجمات الفضاء الالكتروني عسكريا او سياسيا في أي صراع أقرب إلي توصيفها بالإرهاب عن كونها حربا، ولا يحمل ذلك تقييما أخلاقيا لها بقدر ما هو تعبير عن طبيعتها الفنية وطرق حدوثها، ويتحرك ذلك من معطيات تتعلق باعتمادها علي الترويع وبث الخوف وعدم معلومية مصدرها، ولا بالحجم الفعلي للخسائر، ولا بمعرفة الكيفية التي تم بها الهجوم.وتدخل في إطار الحروب غير المتكافئة، كون الطرف الذي يتمتع بقوة هجومية ويبادر باستخدامها هو الطرف الأقوي، بغض النظر عن حجم قدراته العسكرية التقليدية،وهو ما يؤثر في نظريات الردع الاستراتيجي.ولا تستطيع أن تميز هجمات الحرب الالكترونية بين ما هو منشآت مدنية والأخري ذات الطبيعة العسكرية وهو ما يصعب معه فرض الحماية الدولية.[2]

ومن ثم تقف عملية استخدام مصطلح"الحرب "او" الارهاب "، لوصف الاعمال العدائية عبر الفضاء الالكتروني على طبيعة الاستخدام السياسي وتوظيفها دعائيا بين الدول، فعلى سبيل المثال وصفت ايران تعرضها

[1] ـشمويل أيفين ودافييد سيمان توف، **حرب الفضاء الالكتروني**، المفاهيم والاتجاهات، برلين، 2012
[2] عادل عبد الصادق، **نفس المرجع السابق**، ص 35 ، 40

لهجمات فيروس "ستاكس نت" عام 2010 بانها عملا ارهابيا ، بينما وصفت الولايات المتحدة الهجوم الالكتروني على شركة "سوني" الكورية بانها ارهابا الكترونيا تمارسه كوريا الشمالية .[1]

و صدر عن شبكة "Security Week" أواخر كانون الأول/ ديسمبر، لائحة تضمّ أسوء خروقات البيانات التي شهدها العام 2014.

وبحسب ما اعلنه "مركز موارد إنتحال الهوية" (Center Identity Theft Resource)، زاد عدد خروقات البيانات في العام 2014 بنسبة أكثر من 25% مقارنةً بالعام 2013.

وفي ما يلي لائحة بأسوأ خروقات البيانات التي شهدها العام 2014:

1- إختراق موقع المزاد العالمي الإلكتروني Ebay:

تمّ اختراق هذا الموقع في الفترة الزمنية الممتدة بين أواخر شهر شباط/فبراير الماضي وبداية شهر آذار/ مارس، وقد سيطر القراصنة الإلكترونيون على أوراق إعتماد الدخول الخاصة بالموظفين، ومن ثم وصلوا إلى قاعدة بيانات تتضمّن سجلات المستخدمين، الأمر الذي دفع إدارة الموقع إلى الطلب من مستخدميه الذي بلغ عددهم 145 مليون تغيير كلمات السر الخاصة بهم. وتضمنت قاعدة البيانات عناوين البريد الإلكتروني وتواريخ الولادة وكلمات السرّ المشفّرة.[2]

وشكل هذا الخرق تركيزاً على أهميّة إثبات الأصالة المتميزة بعاملين، بالنسبة للموظفين والعملاء على حدّ سواء.

2- إختراق مؤسسة ""JP Morgan Chase المالية الرائدة:

بدأ هذا الإختراق بخادم (Server) استخفّت الشركة بحمايته، وبعد استهدافه، تمكن القراصنة من التحرّك داخل الشبكة وبالتالي الوصول إلى حوالي 90 خادم آخر. وفي حين أنّه لم يكن هناك بيانات مالية تأثرت بالأمر، إلا أنّ القراصنة تمكنوا من الوصول إلى سجلات العملاء التي كشفت عن عناوين بريدهم الإلكتروني وأرقام هواتفهم المنزلية وعناوينهم البريدية (76 مليون عميل منزلي و7 مليون عميل تجاري).

3- إختراق موقع "Home Depot":

بلغ مجموع السجلات المستهدفة في هذا الخرق 56 مليون بطاقة دفع و33 مليون عنوان بريد إلكتروني

---

[1] الهجمات السيبرانية :**مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر** مجلة المحقق الحلي للعلوم القانونية والسياسية العدد الرابع /السنة الثامنة 2016.

[2] ايهاب شوقي، **الحرب السيبرانية...حرب المستقبل المفزعة**، مقال منشور على الانترنت (مصدر) تاريخ الدخول: 2018/02/05 http://www.anntv.tv/new/showsubject.aspx?id=101954

للعملاء. وقد بدأ الهجوم عبر سرقة أوراق إعتماد المستخدمين التي كان يملكهم طرف ثالث بائع. وبعد إستخدام أوراق الإعتماد كوسيلة لتحقيق هذا الإختراق، تمكن المهاجمون من زيادة الإمتيازات والوصول إلى أجزاء من شبكة الموقع، ونشر البرمجيات الخبيثة المبنية خصيصاً على الأنظمة الذاتية للدفع، والموجودة إجمالاً في الولايات المتحدة الأميركية وكندا.

تجدر الإشارة إلى أنّ القراصنة استخدموا في هذا الإختراق نقطة ضعف موجودة في نظام Windows والتي تخلّصت منها الشركة بعد حدوث الإختراق.

4- إختراق أنظمة المستشفيات:

أثر هذا الخرق على أرقام الضمان الإجتماعي، إضافةً إلى سرقة أسماء وعناوين حوالي 4.5 مليون مريض. وقد استخدم القراصنة في هذا الخرق نقطة ضعف أيضاً، الأمر الذي ألقى الضوء على أهميّة إدارة الثغرات وتحديد الاولويات في ما يتعلق بالإصلاحات.

5- إختراق موقع "Staples":

ونتج هذا الإختراق عن نشر البرمجيات الخبيثة في 115 من محلات البيع بالتجزئة، والتي أثرت على 1.16 بطاقة دفع، وذلك عبر الحصول على بيانات عمليات الشراء التي حصلت.

اشهر النماذج:

تقول تاتيانا أنانوف ان الأمن السيبراني عاد ليحتلّ قائمة الأخبار في العالم، وليشغل بال السلطات والادارات موضوع إعادة النظر في كيفيّة تحصين بياناتهم السيبرانية ضدّ أي هجومٍ عليها.

ففي أوائل أواخر تشرين الثاني/نوفمبر الماضي، اكتشفت شركة SONY أنها تتعرّض للقرصنة، حيث تمّ سرقة بيانات تحتوي على معلوماتٍ شخصية تتعلّق بموظفي الشركة، الرسائل الإلكترونيّة التي ترسل فيما بينهم، بالإضافة إلى معلومات حول رواتب التنفيذيين في الشركة ونسخاً لأفلام من إنتاج SONY لم يتم الكشف عنها بعد.

والملفت في هذا الهجوم، أنّ هدفه لم يكمن في سرقة بيانات بغية الإبتزاز للحصول على الأموال على سبيل المثال، بل في منع إطلاق فيلم "Interview The" من إنتاج الشركة، وهو فيلم كوميدي يدور حول مؤامرة لاغتيال الزعيم الكوري الشمالي كيم جونغ أون.[1]

كان الهدف من هذا الهجوم إذاً سياسياً.

[1] نفس المرجع، ايهاب شوقي، **الحرب السيبرانية...حرب المستقبل المفزعة**، مقال منشور على الانترنت: تاريخ الدخول: 2018/02/08 http://www.anntv.tv/new/showsubject.aspx?id=101954

أطلق المهاجمون على نفسهم إسم "حراس السلام" أو "GOP"، وبحسب التقديرات فإنّ الهجوم بدأ منذ أكثر من سنة، حيث سيطر القراصنة على أكثر من 100 تيرابايت من البيانات الخاصة بـSONY.

ولم يقتصر الأمر على ذلك فحسب، فقد نشر القراصنة برمجية خبيثة تسمّى بـWiper، وهي مصممة لمحو البيانات من الخوادم.

ونتيجةً للأمرين، تعطّلت أجهزة كمبيوتر خاصة بموظفين في الشركة، كما تم السيطرة على حسابات Twitter مختلفة تابعة لـSONY.

وفي السياق نفسه، أطلق "حراس السلام" تهديدات إرهابية وأخرى تتعلق بحوادث 11 أيلول/ سبتمبر 2001، الأمر الذي أدّى أخيراً إلى تدخّل مكتب التحقيقات الفدرالي (FBI) في الأمر وفتح تحقيق.

وتصاعدت التكهنات حول ما إذا كانت كوريا الشمالية مسؤولة عن هذا الهجوم، بخاصة بعدما وصف متحدّث باسم وزارة الخارجية الكورية الشمالية في حزيران/يونيو الماضي الفيلم بالإرهابي، متوعداً بانتقام "غير رحوم" إذا ما تمّ عرضه في صالات السينما، غير أنّ كوريا الشمالية لا تزال تنفي حتّى اليوم مشاركتها، مثنيةً من جهّةٍ أخرى على الهجوم ومعتبرةً أنه "عمل صالح".

والملفت أيضاً في هذا الهجوم أنّه كان لصالح القراصنة، حيث تمّ التراجع عن عرض الفيلم الذي كان من المفترض إطلاقه في 25 ديسمبر الماضي.

في هذا الإطار، أشار العميد المتقاعد جاك باكاييف، الذي أنهى خدمته في قوى الأمن الداخلي – شعبة المعلوماتية – وهو استشاري في شؤون المعلوماتية وأمن المعلومات، أنّ هذا الحادث سيسلّط الضوء على مسائل أخلاقيّة كنشر المعلومات السرية المسروقة من قبل الصحف، وقانونيّة وبخاصةٍ حول ما إذا كان للإعلام الحق في نشر معلوماتٍ سريّة أخلاقية. وقد شدّد باكاييف على أهميّة تأمين المعلومات وضرورة تطوير الشركات منصّة موثوقة يخزّن فيها المعلومات احتياطياً، حتى لا يتم فقدان أي معلومات هامّة وأساسيّة للعمل، كما يجب توخّي الحذر عند إرسال الرسائل الإلكترونية.

وقد أدّى الهجوم السيبراني على شركة SONY إلى إعلان الرئيس الأميركي باراك أوباما في منتصف كانون الثاني/يناير الجاري، عن تبنى الكونغرس تشريعات جديدة، من أجل تعزيز تبادل المعلومات بين القطاع الخاص والحكومة – وذلك لمكافحة التهديد الإلكتروني – وإعادة إحياء القانون المتعلّق باستخدام الكومبيوتر لأعمال إحتيال الذي صدر في العام 1984، والذي يحدّد أيضاً متى وبماذا يمكن اتهام قراصنة الإنترنت.

بالإضافة إلى ذلك، ألزم البيت الأبيض الشركات الأميركية، تحت طائلة القانون، تحذير الزبائن عن خطرٍ ما في حال تعرّض شبكاتها للخطر، واقترح الرئيس الاميركي أيضاً إصدار قواعد جديدة لحماية البيانات.

وبحسب باكاييف، تمّ في الأساس الإشتباه بكوريا الشمالية في عملية قرصنة SONY، نظراً لأنّ الفيلم كان متعلّقا بكوريا الشمالية، ونظراً لأنّ التقنية المستخدمة مشابهة للطريقة التي يستخدمها عادةً الجيش السيبراني الخاص بكوريا الشمالية.[1]

[1] ايهاب شوقي، **نفس المرجع السابق**

تجدر الإشارة إلى أنّ حساب القيادة المركزية الأميركية (CentCom) تعرّض للهجوم أيضاً، من قبل قراصنة ينتمون إلى تنظيم داعش، وأصبحت الهجمات السيبرانية واقعًا ملموسا يهدد شبكة الإنترنت كلّها.

وفي ما يتعلق بمستقبل العالم السيبراني، اعتبر باكاييف أنّه نظراً لازدياد البيانات، ستزداد بالتالي التهديدات والهجومات السيبرانية، وسوف يستمر القراصنة بعملهم وذلك يرتبط إجمالاً بصعوبة اكتشافهم.

وأضاف أنّه في هذا العصر، توازي المعلومات المال والذهب من حيث القيمة، لذلك يجب تأمينها بأفضل الطرق.

وقد توافقت المملكة المتحدة والولايات المتحدة الأميركية على اعتبار التهديدات السيبرانية واحدة من أهم وأخطر التحديات التي يواجهها العالم اليوم، ولذلك يجب إعادة هيكلة طرق تأمين البيانات والإنترنت بشكلٍ عام، بدءاً من البنى التحتية الخاصّة بها، إلى تطوير برمجيات أكثر تعقيداً تمنع الإختراقات السيبرانية المختلفة.

تعدّت إذاً الهجمات السيبرانية وجهتها الأساسية، التي كانت تهدف إلى سرقة بيانات لتتمكن من سرقة أموال بطريقة سهلة وسلسة، وأصبحت ذات طابعٍ سياسي، تهدف إلى نشر الخوف والإرهاب في بعض الأحيان، أو إلى تثبيت القدرات في أحيانٍ أخرى.

تجدر الإشارة إلى أن أوّل عملية ذات طابعٍ سياسي تعود إلى العام 2010، عندما تم اكتشاف برمجيّة خبيثة نشرت على أجهزة كمبيوتر ايرانية، وذلك لإلحاق الضرر بأجهزة الطرد المركزي لتخصيب اليورانيوم في بعض المنشآت النووية الإيرانية، ويعتقد الخبراء أنها من صنع الولايات المتحدة الأمريكية وإسرائيل.

رعب في اسرائيل:

وفي العام الماضي، نشر موقع ״يسرائيل ديفينس״ المتخصص في الشأن العسكري الإسرائيلي، تقريره عن استطلاع للرأي أجراه معهد ״IPS״ للدراسات السياسية والاستراتيجية وذلك قبيل انعقاد المؤتمر الرابع عشر لمستوطنة ״هرتسليا״ والذي سيركز في موضوعاته على التهديد الإلكتروني ״حرب السايبر״ التي تهدد المجتمع الإسرائيلي.

ومن خلال السؤال الذي طرحه المعهد على الأشخاص الذي أجرى عليهم الاستطلاع تبين أن حوالي 62% منهم يروا أن هناك خطر حقيقي وأساسي على إسرائيل جراء ״ حرب السايبر״ وكان السؤال الذي تم طرحه هو، هل ترى أن تهديد ״ حرب السايبر״ يمثل خطراً وتهديداً من التهديدات على الأساسية على دولة إسرائيل؟ وكانت إجابة أكثر من 62% بنعم، حيث يرون أن ״حرب السايبر״ هي الخطر القادم على إسرائيل.

وأشار الموقع إلى حجم الخوف المسيطر على المجتمع، حيث أن نسبة الـ 62 % التي أكدت الخطر على إسرائيل كانت من إجمالي حوالي 65 % ممن أجري عليهم الاستطلاع يتضح من خلال الاستطلاع الذي تم أجراؤه على حوالي 500 فرد أن نسبة من يرون ״ حرب السايبر״ لا تمثل خطراً كانت أقل ممن يرون فيها خطراً

حقيقا على وجود إسرائيل، اذ بلغت نسبتهم حوالي 29% فقط، وأشار التقرير إلى أن معظم الخائفين كانوا من المتدينين وليس العلمانيين، وألمح الموقع أن هذا يعود إلى فارق الثقافة بين الطائفتين في إسرائيل.

وحسب تقرير نشره موقع " المركز الفلسطيني للإعلام" فإن حرب السيبر تمثلاً فزاعة وخطراً كبيراً على إسرائيل حيث قال قائد شعبة الاستخبارات العسكرية الجنرال، أفيف كوخافي، في المؤتمر السنوي لـ"مركز دراسات الأمن القومي" أن "حرب السايبر" باتت، في نظره، أهم من اكتشاف البارود.

وأضاف كوخافي أنه في عام 2013 نفذ الكثير من الهجمات الإلكترونية على مؤسسات ومواقع الكرتونية تابعة للجيش الإسرائيلي، وأكد أن مجال حرب السايبر مازال في البداية وأن هناك تطورات خطيرة تنتظره في المستقبل، وأكد على الطفرة التي أحدثتها حرب السايبر حيث في الماضي كان يلزم لجمع معلومات استخباراتية مثلاً عشرة أشخاص الآن وبعد التطور في هذا المجال يمكننا أن نقوم بتلك المهمة من خلال شخص واحد فقط.

وفي سياق متصل نجد المسئول الأول عن شعبة التكنولوجيا في إسرائيل يحذر من الخطر الذي يداهم إسرائيل من قبل القرصنة الإلكترونية والحرب السيبرية ، وأكد على ضرورة إنشاء قيادة مستقلة لحرب السايبر.[1]

[1]ايهاب شوقي، **نفس المرجع السابق**

المبحث الثاني:دور القانون الدولي في تجريم القرصنة والحرب السيبيرانية:

نشر مجموعة من الخبراء القانونيين والعسكريين مؤخرًا دليلاً يعرف بـ "دليل تالين" يشير إلى أن القانون الدولي الإنساني ينطبق على الحرب السيبرانية ويحدد الدور الذي ستلعبه قواعد القانون الدولي الإنساني في هذا المجال.

يقدم "دليل تالين" رؤىٍ مثيرة للاهتمام في هذا الصدد. فهو يتمسك على سبيل المثال بالثنائية التقليدية للنزاعات المسلحة الدولية والنزاعات المسلحة غير الدولية، ويقر بأن العمليات الإلكترونية وحدها قد تشكل نزاعات مسلحة تبعاً للظروف – لا سيما الآثار المدمرة لتلك العمليات. ويقدم الدليل في هذا الصدد تعريفاً "للهجوم السيبراني" بموجب القانون الدولي الإنساني بوصفه "عملية إلكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها". ويكمن صلب الموضوع مع ذلك في التفاصيل أي ما ينبغي أن يُفهم على أنه "ضرر" في العا لم الالكتروني. وبعد مناقشات مكثفة، اتفق أغلب الخبراء على أنه علاوة على الضرر المادي فإن توقف أحد الأعيان عن العمل قد يشكل ضرراً أيضاً. وتتمثل وجهة نظر اللجنة الدولية في أنه إذا تعطل أحد الأعيان، فليس من المهم كيفية حدوث ذلك سواء بوسائل حركية أو عملية إلكترونية. وهذه القضية مهمة للغاية في الممارسة العملية حيث أن أي عملية إلكترونية تستهدف تعطيل شبكة مدنية خلاف ذلك، لن يشملها الحظر الذي يفرضه القانون الدولي الإنساني على الاستهداف المباشر للأشخاص المدنيين والأعيان المدنية.[1]

ما هو الدور الذي اضطلعت به اللجنة الدولية في هذه العملية؟ وهل انعكست مواقفها في الدليل؟

لقد ساهمت اللجنة الدولية بصفة مراقب في مناقشات الخبراء الذين صاغوا دليل "تالين" لضمان انعكاس القانون الدولي الإنساني القائم في الدليل بأقصى قدر ممكن، وتعزيز الحماية التي يوفرها هذا الفرع من القانون لضحايا النزاعات المسلحة. وتعكس القواعد الخمس وتسعون المدرجة في الدليل النصوص التي حظيت بإجماع في الرأي بين الخبراء. وتتفق اللجنة الدولية بشكل عام مع صيغة القواعد، ولكن قد توجد بعض الاستثناءات، فعلى سبيل المثال لا تشمل القاعدة التي تذكِّر بحظر اقتصاص الأطراف المتحاربة من عدد من الأشخاص والأعيان التي تتمتع بحماية خاصة الممتلكات الثقافية، على عكس ما توصلت إليه دراسة اللجنة الدولية الخاصة بالقانون الدولي الإنساني العرفي من نتائج. ويقدم الدليل أيضًا تعليقات مفيدة على القواعد تشمل التعبير عن وجهات نظر متباينة بين الخبراء. وأحد الأمثلة على هذا التباين يخص التزام أطراف النزاع المسلح باتخاذ جميع الاحتياطات الممكنة لحماية السكان المدنيين والأعيان المدنية الواقعة تحت سيطرتها من آثار الهجمات السيبرانية: فبينما يشير التعليق الوارد في الدليل إلى أن نطاق تطبيق هذه القاعدة يقتصر على النزاعات المسلحة الدولية، تعتبر اللجنة الدولية هذا الالتزام منطبقاً على أي نوع من أنواع النزاعات المسلحة.[2]

[1] محمد أمين الروس، "جرائم الكمبيوتر و الانترنت"، (الاسكندرية: دار المطبوعات الجامعية، 2004) ص 30،31.
[2] محمد حماد الهيتي، "جرائم الحاسوب"،ط1 (عمان: دار المناهج، 2006) ص 163.

ما هي التحديات الأساسية التي تثيرها الحرب السيبرانية؟

يوجد فضاء إلكتروني واحد فقط تتقاسمه القوات المسلحة مع المستخدمين المدنيين وكل شيء فيه متشابك ومترابط. وتتمثل التحديات الرئيسية في ضمان توجيه الهجمات ضد الأهداف العسكرية فقط، وتوخي الحرص بشكل مستمر لحقن دماء السكان المدنيين والبنية التحتية المدنية. علاوة على ذلك لا يجب أن تكون الإصابات العرضية المحتملة في صفوف المدنيين والأضرار مفرطة مقارنة بالميزة العسكرية المباشرة والملموسة المتوقعة من الهجوم السيبراني. و إذا لم تُستوفى هذه الشروط، لا ينبغي شن الهجوم. ويستحضر الدليل في هذا الصدد وبشكل مناسب أن الأضرار العرضية تتضمن الآثار المباشرة وغير المباشرة، وأن أي آثار غير مباشرة متوقعة ينبغي أن تُدرج في تقييم التناسب أثناء عملية التخطيط للهجوم وتنفيذه، وهي نقطة ذات صلة كبيرة بالفضاء الالكتروني. وتؤكد هذه التحديات على أهمية توخي الدول الحذرالشديد عند اللجوء إلى الهجمات السيبرانية.

هل القراصنة هدف مشروع في الحرب السيبرانية؟

يشمل مصطلح "القراصنة" الكثير من الأشخاص المنخرطين في أنشطة مختلفة بدرجة إلى حد لا يمكن في إطاره القول بأن القراصنة بصفتهم تلك يمكن أن يكونوا محلاً للهجوم. ولا تتصل معظم العمليات الإلكترونية بنزاع مسلح، ومن ثم فإن القانون الدولي الإنساني لا يطبق عليها. وحتى في النزاع المسلح، يُعتبَر معظم القراصنة مدنيين يستمرون في التمتع بحماية القانون الدولي الإنساني من الهجوم المباشر عليهم، رغم أنهم يظلون خاضعين لعمليات إنفاذ القانون وقد يتعرضون للمقاضاة الجنائية تبعاً لما إذا كانت أنشطتهم تنتهك مجموعة أخرى من القوانين.

ولكن الوضع يختلف إذا شارك القراصنة بشكل مباشر في العمليات العدائية من خلال هجمات سيبرانية لدعم أحد طرفي النزاع المسلح. ففي هذه الحالة لا يتوقع القراصنة أن يظل العدو ساكنًا، وهم يخسرون الحماية القانونية المكفولة لهم ضد الهجوم المباشر أثناء تنفيذ الهجوم السيبراني والإجراءات التحضيرية التي تشكل جزءًا لا يتجزأ من هذا الهجوم.

هل يمكن استخدام التكنولوجيا السيبرانية بشكل إيجابي أثناء النزاعات المسلحة؟

يقع على عاتق الدول أثناء سير العمليات الحربية التزام بتجنب الإصابات العرضية في صفوف المدنيين والإضرار بالبنية التحتية المدنية أو الحد منها على أقل تقدير. ودون التقليل من شأن التحديات، لا يمكن للمرء استبعاد إمكانية أن يؤدي التطور التكنولوجي في المستقبل إلى تطوير أسلحة سيبرانية من شأنها التسبب في إصابات وأضرار عرضية أقل من الأسلحة التقليدية في ظروف معينة، لتحقيق الميزة العسكرية نفسها. وسوف تواصل اللجنة الدولية رصد التطورات في هذا الصدد.

القرصنة من وجهة نظر القانون:

المصطلح القانوني:

هناك عدة مصطلحات يمكن ان تستخدم للتعبير عن الظاهرة الجرمية الناشئة في بيئة الحواسيب الالكترونية والشبكات كسوء الاستخدام ، الاحتيال ، الجريمة المعلوماتية ، جرائم القرصنة ، الاختراق وجرائم الانترنيت.

واختيار المصطلح يتعين بارتباط البعدين التقني والقانوني ، فاذا عدنا للحقيقة الاولى المتصلة بنشأة وتطور تقنية المعلومات نجدها تشمل فرعين جرى بحكم التطور تقاربهما واندماجهما هما الحوسبة والاتصالات ، فتقوم الحوسبة على استخدام التقنية لأدارة وتنظيم ومعالجة البيانات في اطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق ، اما الاتصال فقائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها الدارجة[1].

يتبين لنا من ذلك ان من الصعوبة ايجاد مصطلح شامل يعبر عن كل الحالة الجرمية المرتكبة التي يقوم بها المخترقون ، فاذا وصفنا جريمة معينة بأنها جريمة اتصالات فليس بالضرورة ان تكون مرتبطة بالحاسوب او الانترنيت وانما مقتصرة على سرقة خطوط هاتفية مثلاً ، واذا وصفنا حالة اخرى بأنها جريمة حاسوب فليس بالضرورة ان يكون لها علاقة بأجهزة الاتصال وانما قد تكون زرع برنامج فايروس في حاسوب ما.

لذا يجب ان يكون المصطلح المستخدم لوصف جرائم المعلوماتية شاملاً لمعنى الجريمة بكل تفاصيلها وتفرعاتها.

القرصنة في تشريعات بعض دول العالم:

لو بحثنا في تشريعات دول العالم المتطورة لوجدنا الكثير من النصوص التي تعاقب جرائم القرصنة واختراق الانظمة الالكترونية ، بينما لا تزال دول اخرى كثيرة تعيش في ظلام الكتروني دامس لذا لا نرى أي تشريع يخص هذا النوع من الجرائم ، وساذكر في هذا الفصل التشريعات الصادرة في بعض دول العالم[2].

السويد:

تنص المادة (21) من القانون المرقم (289 (والصادر في 2 نيسان 1973 الخاص بالبيانات على ان ((يعاقب كل من ولج بوسائل غير مشروعة الى سجل مخصص لمعالجة البيانات آلياً)) من هذا يتبين ان القانون السويدي يعاقب لمجرد الولوج غير المشروع.

[1] عبد الله علي عبد الله، **تقنيات الاختراق المادي**، دار البشائر الإسلامية–بيروت،ط1، 2003،ص 144 – 146 .

[2] محمد عبد الله المنشاوي: **جرائم الانترنت من منظور شرعي و قانوني**، بحث منشور على الانترنت (مصدر) تاريخ الدخول 2018/02/15 www.minshawi.com

الدنمارك:

طبقاً للمادة (263) من القانون الصادر في ١ حزيران 1985 – يعد من قبيل الجرائم فعل الولوج في المعلومات او البرامج المخزونة في الحواسيب.

فرنسا:

استحدث القانون الفرنسي الصادر في 5 كانون الثاني 1988 بموجب المادة (462) الفقرة الثانية من قانون العقوبات ، جريمة الولوج غير المشروع في نظم المعلومات والتي تم تعديلها بموجب القانون الصادر في 29 آذار 1993 في المادة (331) الفقرة الاولى من قانون العقوبات والتي نصت ((يعاقب بالحبس لمدة سنة واحدة وبغرامة تصل الى مائة الف فرنك كل من تواجد او بقى على نحو غير مشروع في نظام معالجة آالية سواء على نحو كلي او جزئي . وتشدد العقوبة بالحبس لمدة سنتين وبغرامة مقدارها (200.000 فرنك اذا ما ترتب على ذلك الغاء او تعديل للبيانات التي يحتويها هذا النظام او باختلاف وظيفة هذا النظام.[1]

انكلترا:

في عام 1990 تم استحداث قانون يعالج فيه اساءة استخدام نظم المعلومات وقد تم بموجب هذا التشريع تجريم عملية دخول أي فرد على البياتات المخزونة في الحاسوب او البرامج وكذلك عملية تعديلها بصورة غير مشروعة او أي محاولة لفعل ذلك[2].

وقد نص القانون على ثلاث جرائم وهي-:

1- الدخول المتعمدْ غير المشروع.

2- الدخول غير المشروع والذي يتم بنية ارتكاب العديد من الجرائم.

3- القيام بأي فعل متعمد ينشأ عنه اجراء تعديل غير مشروع لمحتويات اجهزة الحاسوب.

الولايات المتحدة الامريكية:

صدر قانون الولوج المصطنع في الحاسب الآلي في تشرين الاول 1984 والذي يعاقب من ولج عمداً في حاسوب بدون اذن او كان مسموحاً له واستغل الفرصة التي سنحت له لأغراض لم يشملها الاذن وقام عمداً بواسطة هذه الوسيلة باستعمال او تعديل او اتلاف او افشاء معلومات مخزونة في الحاسوب متى كان هذا الاخير يعمل لصالح الحكومة الامريكية وطالما اثرت هذه الافعال على اداء وظيفته[3].

---

[1] Oona` A.Hathway , Rebecca Crootof , Philip Levtiz , aley Nix, Aileen Nowlan ,William Perdue and Julia Spiegel, "**The Law of Cyber –Attack**", California Law Review, 2012 ,p7.

[2] عبد الله علي عبد الله، **نفس المرجع السباق**، ص 144 – 146

[3] محمد عبد الله المنشاوي، **نفس المرجع السابق**.

دور قوانين الحماية الفكرية في بعض البلدان العربية:

قد يكون لتأخر استخدام تقنيات الحاسب الالي في الدول العربية قياساً بباقي دول العالم الاثر الكبير لتأخر اصدار تشريع يخص توفير حماية قانونية لبرامج الحاسوب من السرقة والاختراق.

الا ان اغلب الدول العربية اهتمت كثيراً بقوانين الحماية الفكرية حتى ان بعضها قد ساهم وبشكل كبير في الجهد الدولي لحماية الملكية الفكرية اعتباراً من القرن التاسع عشر.

شهدت خمسينيات القرن الماضي موجه واسعة من التشريعات التي تهتم بحماية براءات الاختراع والعلامات التجارية والتصاميم الصناعية , وكانت فترة الثمانينات قد شهدت اصدار التشريعات التي تخص حماية حق المؤلَف والحقوق المجاورة . اما فترة التسعينات فقد شهدت اقرار قوانين او تعديل قوانين سابقة لتشمل برامج الحاسوب وقواعد البيانات . وفيما يلي بعض الامثلة على هذه التشريعات[1].

العراق:

صدر امر سلطة الائتلاف رقم (83) لسنة 2004 وهو تعديل لقانون حق المؤلَف رقم (3) لسنة 1971 حيث تضمنت احدى فقراته)برامج الكومبيوتر , سواء برمز المصدر او الالة التي يجب حمايتها كمصنفات ادبية.

مصر:

في القانون رقم (38) لسنة 1992 وهو تعديل للقانون المرقم (354) لسنة 1954 اصبحت فيه الحماية الفكرية تشمل مصنفات الحاسب الالي من برامج وقواعد بيانات وما يماثلها.

الامارات:

نص القانون رقم (40) لسنة 1992 المادة الثانية (يتمتع بالحماية الفكرية المقررة في هذا القانون مؤلفو المصنفات الفكرية المبتكرة في الاداب والفنون والعلوم – وشملت الفقرة (ز) من هذا القانون برامج الحاسوب

الاردن:

ورد في قانون حماية المؤلَف رقم (22) لسنة 1992وتعديلاته للاعوام 1998 و 1999و2001 الحماية القانونية للمصنفات الادبية والفنية كما وضمنت بموجبه حماية برامج الحاسوب وقواعد البيانات[2]

---

[1] مروة زين العابدين صالح، **الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولى الاتفاقى و القانون الوطنى**، مركز الدراسات العربية للنشر و التوزيع، ط1، 2016

[2] عبد الله علي عبد الله، **تقنيات الاختراق المادي**، دار البشائر الإسلامية–بيروت،ط1، 2003 ص 144 – 146

لبنان:

في القانون المرقم (2385) لسنة 1924 المعدل بموجب القانون رقم (75) لسنة 1999 يحمي بموجبه جميع انتاجات العقل البشري والتي حددتها المادة الثانية ببرامج الحاسب الالي مهما كانت لغاتها بما في ذلك الاعمال التحضيرية.

يوماً بعد يوم تزداد مخاطر الجرائم المعلوماتية وتتوسع دائرتها لتشمل كافة مرافق الحياة العامة وبدأت تهدد الاقتصاد العالمي نتيجة الخسائر الكبيرة الناتجة عنها , واخطر ما في الامر ان اغلب مرتكبي هذه الجرائم يبقون مجهولي الهوية وهذا الامر يتيح لهم الاستمرار والتفنن بطرق التلاعب بموارد الاخرين عن طريق السيطرة على أنظمتهم الالكترونية.

وما يدعوا للقلق ان الكثير من البلدان ومنها العراق لا يملك لحد الان تشريعاً صريحاً يجرم ظاهرة القرصنة مع وجود بعض المحاولات لاصدار قانون عربي موحد يخص جرائم المعلوماتية بكافة تفرعاتها وقد يكون سبب تأخير اصدار مثل هكذا تشريع يعود لعدم وجود دعاوى قضائية في محاكم العراق كافة ضد مرتكبي جرائم القرصنة والاختراق , وهذا لا يعني عدم وجود جرائم معلوماتية بل ان عدداً غير قليل من المواقع الالكترونية العراقية تتعرض للهجوم سنوياً وخصوصاً مواقع وكالات الانباء والمواقع الحكومية , وان سبب عدم رفع الدعاوى يعود لصعوبة معرفة الفاعل.

لذا يجب وضع دراسة مستقبلية لما قد يحصل جراء تطور هذه الجرائم خصوصاً في هذه المرحلة التي يقبل فيها بعض الدول العربية على تنفيذ مشروع الحكومة الالكترونية وقد بدأت بالفعل بعض الوزارات بالخطوات الاولى لتنفيذ هذا المشروع الامر الذي يستدعي الاسراع بإصدار قوانين صارمة تردع أي شخص يحاول العبث بالوثائق الرسمية[1].

[1] عبد العالي الديربي، محمد صادق اسسماعيل، **الجرائم الإلكترونية"دراسة قانونية قضائية مقارنة"**، المركز القومي للإصدارت القانونية،ط1، 2012.

المبحث الثالث: ظاهرة ويكليكس و القرصنة الروسية للإنتخابات الأمريكية الأخيرة

حملة 2016 الرئاسية التقطيع حقائق سريعة

(CNN)فيما يلي نظرة على حوادث القرصنة خلال حملة الانتخابات الرئاسية لعام 2016 والتدخل الروسي في الانتخابات .للحصول على تفاصيل حول التحقيقات في القرصنة والجهود المبذولة للتدخل في الانتخابات ، راجع 2016 حقائق سريعة حول التحقيق في الانتخابات الرئاسية[1]

الجدول الزمني:

سبتمبر 2015 – اتصل مكتب التحقيقات الفيدرالي بمكتب المساعدة التابع للجنة الوطنية للحزب الديمقراطي ، وحذر قسم تكنولوجيا المعلومات من أن جهاز كمبيوتر واحد على الأقل قد تم اختراقه من قبل المتسللين الروس. يقوم أحد الفنيين بمسح النظام ولا يجد أي شيء مريبًا.

نوفمبر – 2015

مكتب التحقيقات الفيدرالي (FBI) يمد يده إلى DNC مرة أخرى ، محذراً إياهم من أن أحد أجهزة الكمبيوتر الخاصة بهم ينقل المعلومات إلى روسيا .وتقول إدارة DNC فيما بعد إن تقنيي تكنولوجيا المعلومات فشلوا في تمرير الرسالة التي تفيد بأن النظام قد تم اختراقه.

19(مارس) 2016

يتلقى رئيس حملة كلينتون ، جون بوديستا ، بريدًا إلكترونيًا للتصيد الاحتيالي مُلهمًا كتحذير من Googleحاول مستخدم آخر الدخول إلى حسابه .يحتوي على رابط إلى صفحة يمكن لـ Podesta تغيير كلمة المرور الخاصة به .يشارك البريد الإلكتروني مع موظف من مكتب مساعدة الحملة .رد الموظف بخطأ مطبعي – بدلاً من كتابة "هذا بريد إلكتروني غير شرعي" ، اكتب "هذا بريد إلكتروني شرعي ."يتبع Podesta التعليمات ويكتب كلمة مرور جديدة ، مما يسمح للمتسللين بالوصول إلى رسائل البريد الإلكتروني الخاصة به.

12جوان ، 2016 –

أثناء مقابلة على التلفزيون البريطاني ، يقول مؤسس ويكيليكس جوليان أسانج إن الموقع الإلكتروني قد حصل على مجموعة من رسائل كلينتون الإلكترونية وسوف ينشرها.

[1] Frank Trager and Philip Kronenberg (eds.), **National Security and American Society** (Kansas: Kansas University Press, 1973)

14جوان 2016 –

ذكرت صحيفة واشنطن بوست أن المتسللين الذين يعملون لحساب الحكومة الروسية تمكنوا من الوصول إلى نظام الكمبيوتر الخاص بشركة DNC ، وقاموا بسرقة الأبحاث المعادية على Donald Trump وعرض رسائل البريد الإلكتروني الخاصة بالموظفين ومحادثات الدردشة .غير أن الكرملين نفى أن تكون الحكومة مرتبطة بالاختراق ، كما أخبر مسؤول أمريكي شبكة سي إن إن CNN أن المحققين لم يخلصوا بعد إلى أن الحكومة الروسية وجهت الهجوم الإلكتروني.

15 جوان 2016 –

قامت شركة الأمن السيبراني التي استأجرها DNC بنشر إشعار عام على موقعها على الويب يصف هجومًا على شبكة كمبيوتر اللجنة السياسية من قبل مجموعتين مرتبطتين بالمخابرات الروسية .وبحسب هذا المنشور ، قامت مجموعتان تدعمهما روسيا تدعى "الدب المثلج" و "الدب الفارغ" بنقل نظام الكمبيوتر الخاص باللجنة . رداً على ذلك ، يدّعي أحد المدونين Guccifer 2.0 أنه قام بمفرده بمهمة الإختراق ، وليس الروس .كدليل ، ينشر مذكّرات DNC الداخلية وأبحاثاً معارضة حول ترامب .علاوة على ذلك ، يدعي Guccifer 2.0 أنه قد مرّ آلاف الملفات إلى ويكيليكس .يقدم ترامب نظريته الخاصة حول أصول الهجوم: مما يوحي في بيان بأن DNCاخترق نفسه ليشتت انتباه فضيحة كلينتون الإلكترونية.

22جويلية 2016 :

قبل أيام من المؤتمر الوطني الديمقراطي ، تنشر ويكيليكس ما يقرب من 20000 بريد إلكتروني تم اختراقها من خادم DNC. وتشمل الوثائق ملاحظات تسيء فيها ديبي فاسرمان شولتز ، رئيسة شركة DNC، إلى إهانة موظفي حملة بيرني ساندرز والرسائل التي تشير إلى أن المنظمة كانت تفضل كلينتون بدلاً من البقاء محايدة .يستقيل واسرمان شولتز في أعقاب التسرب.

25جويلية 2016 :

أعلن مكتب التحقيقات الفيدرالي أنه أطلق التحقيق في اختراق DNC. وعلى الرغم من أن البيان لا يشير إلى أن الوكالة لديها مشتبه به أو مشتبه فيه بعينه ، فإن المسؤولين الأمريكيين يخبرون سي إن إن بأنهم يعتقدون أن الهجوم الإلكتروني مرتبط بروسيا[1].

---

[1]–عادل عبد الصادق، **الانترنت والاتصالات ساحة جديدة للتجسس الدولي**، القاهرة، المركز العربي لأبحاث . الفضاء الالكتروني،2012

27جويلية 2016 :

خلال مؤتمر صحفي ، تحدث ترامب عن استخدام كلينتون لخادم بريد إلكتروني خاص أثناء قيامها بعمل وزيرة الخارجية وتطلب من المتسللين العثور على رسائل البريد الإلكتروني المحذوفة .يقول ترامب: "إذا كنت تستمع إلى روسيا ، آمل أن تتمكن من العثور على 30000 رسالة بريد إلكتروني مفقودة ."يدافع نيوت غينغريتش ، وهو بديل ترامب ، عن ترامب في سقسقة ، رافضًا التعليق بأنه "نكتة."

12أوت 2016:

ينشر المخترقون أرقام الهواتف المحمولة وعناوين البريد الإلكتروني الشخصية لـ Nancy Pelosi وأعضاء آخرين في لجنة الحملة الانتخابية للكونغرس.

1سبتمبر 2016 :

خلال مقابلة مع وكالة بلومبرغ نيوز ، يقول الرئيس فلاديمير بوتين إنه هو والحكومة الروسية ليس لهما صلة بالمتطفلين .ويقول إن هوية الجاني أو الجناة ليست بنفس أهمية محتوى التسريبات ، وفي النهاية كشف المتسللون عن معلومات مهمة للناخبين.

22 سبتمبر – 2016:

أصدر الديمقراطيان ديان فاينشتاين وآدم شيف ، وهما من كبار أعضاء لجان مجلس الشيوخ ومجلس النواب ، بيانًا مشتركًا يعلنان أنه استنادًا إلى المعلومات التي تلقاها أثناء جلسات الإحاطة بالكونغرس ، يعتقدان أن وكالات الاستخبارات الروسية تنفذ خطة للتدخل مع الانتخابات .ويدعون بوتين إلى الأمر بوقف الأنشطة.
26 سبتمبر ، 2016 - خلال مناظرة رئاسية مع كلينتون ، تساءل ترامب ما إذا كان الهجوم الإلكتروني الذي نفذته شركة DNC قد نفذته مجموعة ترعاها الدولة أم قرصان وحيد" .يمكن أن تكون روسيا ، لكن يمكن أن تكون كذلك الصين. كما يمكن أن يكون الكثير من الأشخاص الآخرين. كما يمكن أن يكون شخص ما يجلس على سريره ويزن 400باوند."

نوفمبر 2016 :

على مدى شهر ، ينشر موقع ويكيليكس أكثر من 58000 رسالة تم الاستيلاء عليها من حساب جون بوديستا ، رئيس حملة كلينتون.

06 أكتوبر 2016 :DCLeaks

مجموعة من "المتطوعين" الذين يصفون أنفسهم بأنفسهم وتسعى إلى فضح تأثير المصالح الخاصة على المسؤولين المنتخبين ، تنشر مجموعة من الوثائق المسروقة من كلينتون حليفة كليريشيا مارشال .تم تحديد DCLeaksفي وقت لاحق كواجهة للمخابرات العسكرية الروسية.

07 أكتوبر 2016:

وزارة الأمن الداخلي ومكتب المخابرات الوطنية حول الأمن الانتخابي إصدار بيان decla

تواجه ويكيليكس تحقيقات أمريكية في دورها الانتخابي لعام 2016 وتسريبات وكالة الاستخبارات المركزية:

المصادر:

واشنطن رويترز:

قالت مصادر على صلة بالتحقيقات ان ويكيليكس ومؤسسها جوليان أسانج يواجهون تحقيقات متعددة من جانب السلطات الامريكية بما في ذلك ثلاثة تحقيقات في الكونجرس وتحقيق جنائي اتحادي.

رد فعل أنصار هيلاري كلينتون في مسيرتها الانتخابية الليلة في مانهاتن ، نيويورك. رويترز / لوسي نيكلسون

تقوم لجان المخابرات بمجلس الشيوخ ومجلس النواب وقادة اللجنة القضائية بمجلس الشيوخ بالتحقيق في دور الموقع في حملة الانتخابات الرئاسية الأمريكية عام 2016 ، وفقًا لما ذكرته المصادر التي طلبت جميعًا عدم الكشف عن هويتها والوثائق العامة.

نشرت ويكيليكس رسائل إلكترونية من الحزب الديمقراطي وحساب البريد الإلكتروني الشخصي لجون بوديستا ، رئيس حملة هيلاري كلينتون الرئاسية لعام 2016.

وفي تقرير صدر في كانون الثاني (يناير) ، قالت وكالة الاستخبارات المركزية (سي آي إيه) ، ووكالة الأمن القومي ، ومكتب التحقيقات الفيدرالي ، إن الاستخبارات الروسية قامت بعملية القرصنة ، وأرسلت وكالة الاستخبارات العسكرية الروسية (GRU) بيانات مخترقة إلى ويكيليكس عن طريق وسطاء.

وتحقق لجنة المخابرات بمجلس الشيوخ في من أعطى ويكيليكس بيانات اللجنة الوطنية الديمقراطية التي تم اختراقها والتي نشرتها ويكيليكس في يوليو 2016 ، والتي شملت أكثر من 44 ألف بريد إلكتروني و 17 ألف ملحق ، حسبما ذكرت المصادر .وحتى الآن ، لا تزال تحقيقاتها في مرحلة مبكرة ، حسبما ذكرت المصادر.

طلب قادة اللجنة القضائية في مجلس الشيوخ من جاريد كوشنر ، صهر ترامب ، تلقي رسائل البريد الإلكتروني المتعلقة بـ "ويكيليكس."

استجوبت لجنة الاستخبارات في مجلس النواب روجر ستون ، وهو صديق قديم للرئيس دونالد ترامب ، وعميل سياسي مخضرم روج لإفصاح ويكيليكس عن رسائل البريد الإلكتروني على تويتر.

بعد رفضه في البداية لتحديد وسيط تعامل مع من كان على اتصال مع أسانج ، أخبر ستون اللجنة في وقت لاحق أنه كان راندي كريديكو ، كوميدي يساري.

أرسلت اللجنة رسالة إلى كريديكو تطلب منه الظهور بمحض إرادته .وعندما رفض القيام بذلك ، أرسلت اللجنة إليه مذكرة استدعاء تطلب منه تقديم إفادة.

وقال مارتن ستولر ، محامي كريديكو ، يوم الأربعاء إن كريديكو يدرس إمكانية التمسك بحقوقه الخاصة

بالتعديل الأول والخامس بموجب دستور الولايات المتحدة لتجنب الإجابة عن الأسئلة.

ومن غير الواضح ما إذا كان كريديكو يمكن أن يساعد المحققين في الكشف عن مكان حصول ويكيليكس على رسائل البريد الإلكتروني الديموقراطية التي تم اختراقها.

في رسائل البريد الإلكتروني لرويترز ، رفض ستون استنتاج وكالات الاستخبارات حول القرصنة الروسية.

من غير المعروف ما إذا كان روبرت مولر ، المحامي الخاص لوزارة العدل التي تحقق في احتمال تدخل روسيا في الانتخابات الرئاسية لعام 2016 ، يحقق في ويكيليكس.

وقال محام من الولايات المتحدة لـ Assange ، باري بولاك ، إن فريق Mueller لم يتصل به.

في هذه الأثناء ، يقوم المدعون الفدراليون في الإسكندرية بفيرجينيا بإجراء تحقيق جنائي في كيفية حصول ويكيليكس على الآلاف من وثائق الحكومة الأمريكية السرية ، بما في ذلك مواد وكالة المخابرات المركزية وأحدث المواد التقنية السرية للغاية التي تصف أدوات اختراق أجهزة التجسس الأمريكية .وقالت مصادر إنفاذ القانون وبولاك إن التحقيق بدأ منذ عدة سنوات.

عاش أسانج في سفارة إكوادور في لندن لعدة سنوات بعد أن لجأ إليها عندما طلبت السلطات السويدية تسليمه في قضية تحرش جنسي.

للاتهامات الأمريكية بتدخل روسيا في الانتخابات لصالح ترامب:

أفادت وكالات الاستخبارات الأمريكية بتدخل روسيا في الانتخابات الرئاسة الأمريكية لدعم «دونالد ترامب»، باختراقها لرسائل البريد الإلكتروني للحزب الديموقراطي، ومدير حملة مرشحته «هيلاري كلينتون» في الانتخابات.

وهو اتهام أزعج الرئيس الأمريكي «باراك أوباما»، مهددًا روسيا باتخاذ إجراءات ضدها، فيما أرجعت كلينتون سبب خسارتها في الانتخابات إلى «القرصنة الروسية»، و اعتبر ترامب تلك الاتهامات «سخيفة»، ووصفتها روسيا بأنها »تفوق الوقاحة»، ونفت «ويكيليكس» التورط الروسي بها.

وكالات الاستخبارات الأمريكية: روسيا لصالح ترامب:

و أفادت » وكالة الاستخبارات المركزية الأمريكية» (سي آي إيه)، بأن لديها أدلة كثيرة على وقوف قراصنة روس مرتبطين بالكرملين وراء الهجمات الإلكترونية، والقرصنة المعلوماتية التي طالت حسابات البريد الإلكتروني لكلينتون ومدير حملتها جون بوديستا،[1] وقادة الحزب الديموقراطي[2] ونشر ت على موقع ويكليكس .[3]ولم تفصح «سي آي إيه» عن تلك الأدلة، وقالت: إن هدف روسيا من ذلك، تحويل دفة انتخابات الرئاسة الأمريكية لصالح ترامب، الذي فاز بها في نوفمبر)تشرين الثاني) الماضي.

[1] https://wikileaks.org/podesta-emails/
[2] https://wikileaks.org/dnc-emails/
[3] https://wikileaks.org/-Leaks-.html

ولم تكن «سي آي إيه» وحدها هي التي وصلت لتلك النتيجة؛ إذ تبين أمس الجمعة،دعمها كلًا من «مكتب التحقيق الفيدرالي» (إف بي آي)، ومدير وكالة الاستخبارات الوطنية الأمريكية، وأفادوا بالتدخل الروسي في الانتخابات الأمريكية لصالح المرشح الجمهوري «دونالد ترامب. »

و قال » جون برينان»، مدير «سي آي إيه»، في رسالة لموظفيه في الوكالة «التقيت بشكل منفصل مع مدير الإف بي آي، جيمس كومي ومدير الاستخبارات الوطنية جيم كلابر، وكان هناك إجماع قوي بيننا على نطاق التدخل الروسي في الانتخابات الرئاسية وطبيعته، والقصد منه. »[1]

أوباما يتعهد بالرد:

تسببت تلك النتائج التي توصلت إليها وكالات الاستخبارات الأمريكية بشأن التدخل الروسي لصالح ترامب في الانتخابات انزعاجًا في البيت الأبيض، وقال المتحدث باسمه، الخميس الماضي: إن الرئيس الروسي «فلاديمير بوتين» متورط في الهجمات الإلكترونية.

وفي اليوم التالي تعهد أوباما باتخاذ إجراءات ضد روسيا، قائلًا في مقابلة مع الإذاعة الوطنية العامة الأمريكية «أعتقد أنه عندما تحاول حكومة أجنبية التأثير على نزاهة انتخاباتنا، فإننا نحتاج إلى اتخاذ إجراء، وسنفعل في وقت ومكان نختاره .«ولم يتبقَ لأوباما سوى أسابيع قليلة تفصله عن الخروج نهائيًا من البيت الأبيض، في 20 يناير (كانون الثاني) المقبل، مُضيفًا أن «السيد بوتين يدرك جيدًا مشاعري بشأن هذا الأمر، لأنني تحدثت معه بصورة مباشرة حول ذلك.«

وشهد أمس الجمعة، آخر مؤتمر صحافي لأوباما في هذا العام. وشغل التدخل الروسي المزعوم في الانتخابات الأمريكية اهتمام الكثير من الصحافيين. وكشف أوباما فيه أنه طلب من بوتين في الصين في سبتمبر أيلول (الماضي) وقف عمليات القرصنة ، وقال: إن عدم تنفيذ ذلك »سيؤدي إلى تداعيات خطيرة، مؤكدًا سنرد على عمليات القرصنة بشكل علني، وأيضًا بطريقة لا يعرف بها أحد » .

وحول مدى معرفة بوتين بتلك الهجمات الإلكترونية، قال أوباما: إنه «لا يحدث الكثير في روسيا دون علم بوتين»، مُؤكدًا أن بلاده تعاملت بالشكل الصحيح مع قضية الاختراق الإلكتروني ، وموضحًا أنه «عندما تأكدنا من حدوثه أعلنت وكالة الاستخبارات ذلك»، حاثًّا خليفته في البيت الأبيض، دونالد ترامب، بدعم التحقيقات بشأن التدخل الروسي في الانتخابات الأمريكية.

[1] https://www.independent.co.uk/news/world/americas/donald-trump-election-russia-cia-fbi-comey-clapper-a7480566.html

كلينتون: القرصنة الروسية سبب خسارتي في الانتخابات

وفي نفس السياق، أرجعت هيلاري كلينتون سبب خسارتها في الانتخابات الرئاسية إلى »القرصنة الروسية» ، وقالت، أمس الجمعة، في تصريحات نقلتها صحيفة نيو يورك تايمز الأمريكية: إن «ما حدث ليس هجومًا على شخصي وعلى حملتي فحسب، بل هو هجوم على بلدنا، فهذا الأمر يتجاوز السياسة، ويتعلق بديموقراطيتنا وأمن أمتنا.

ولفتت المرشحة الديموقراطية الخاسرة في الانتخابات الرئاسية، إلى أن بوتين لديه، ما أسمته بـ«حنق شخصي» تجاهها؛ بسبب وصفها للانتخابات البرلمانية الروسية قبل خمس سنوات بـ«المزيفة»، موضحةً «ألقى بوتين اللوم علي عندما استشرى الغضب بين شعبه، وهذا هو الخط المباشر بين ما قاله في ذلك الوقت، وما فعله في تلك الانتخابات»، في الإشارة لانتخابات الرئاسة الأمريكية[1].

ترامب: اتهامات «سخيفة»

وفي المقابل، وصف ترمب، التدخل الروسي في الانتخابات الأمريكية، باتهامات «سخيفة ومثيرة للسخرية، وذات دوافع سياسية»، منتقدًا تقرير «سي آي إيه» في هذا الشأن.

وتساءل مستنكرًا في تغريدة على موقع التدوينات القصيرة، «تويتر»، نشرها الخميس الماضي «إذا كانت روسيا أو أي كيان آخر ينفذون عمليات قرصنة، لما انتظر البيت الأبيض وقتًا طويلًا كي يتحرك؟ لماذا اشتكى فقط بعدما خسرت هيلاري» في انتخابات الرئاسة الأمريكية؟

وتجدر الإشارة إلى أن بوتين كان من أكبر الداعمين لترامب في الانتخابات الأمريكية، وكان من أول المهنئين له عقب فوزه بها في الثامن من نوفمبر (تشرين الثاني) الماضي. و ذكرت" سي إن إن " ، الخميس الماضي، أن مساعد ترامب ذهب إلى موسكو لبحث رفع العقوبات عن روسيا. ولا تتوقف العلاقات بين بوتين وترامب على الجانب الرسمي فقط، إذ أشار أوباما في مؤتمره الصحافي إلى استطلاع رأي أظهر دعم 37% من الجمهوريين لبوتين.

[1] تايتل برس24 /بغداد، مقال منشور على الانترنت (مصدر) تاريخ الدخول: 2018/04/14
https://alqabas.com/455104/

روسيا: اتهامات « فاقت الوقاحة »

في المقابل، جاء رد الفعل الروسي على الاتهامات الأمريكية بشأن التدخل الروسي في مسار الانتخابات الأمريكية، غاضبًا؛ إذ قال المتحدث باسم الكرملين، «دميتري بيسكوف»، أمس الجمعة: إنّه «في هذه المرحلة بات على الأمريكيين، إما التوقف عن التطرق إلى هذا الموضوع (اتهام روسيا بالاختراقات الإلكترونية)، أو تقديم أدلة، وإلا فهذا يفوق الوقاحة.«

وقال »يوري أوشاكوف»، المسؤول بالكرملين، لوكالة أنباء «تاس» الروسية: إن بوتين أوضح موقف روسيا في هذه القضية، في سبتمبر (أيلول) الماضي، على هامش قمة مجموعة العشرين، مُضيفًا «قدمنا إجابة واضحة جدًا، وربما لم تتفق مع ما كان أوباما يُحاول شرحه لنا.«

ويكيليكس تنفي تورط روسيا في القرصنة الإلكترونية:

من جانبها نفت ويكيلكس تورط موسكو في القرصنة الإلكترونية التي طالت الحزب الديموقراطي في الشهور السابقة للاقتراع في الانتخابات الرئاسية، وشدد «كريج موراي«، الدبلوماسي البريطاني السابق الذي يعمل في «ويكيليكس»، على أن ما أسماها بـ«الإدعاءات الأمريكية»، فيما يخص حصول ويكيليكس على رسائل حملة كلينتون من الحكومة الروسية، «لا صدقية لها.«

وأضاف موراي في حديث له مع صحيفة «ديلي ميل «البريطانية أن «أحد أعضاء الحزب الديمقراطي هو من سلم إلى ويكيليكس رسائل أعضاء اللجنة الوطنية للحزب الديمقراطي، كما سلم رسائل مدير حملة كلينتون الانتخابية جون بوديستا؛ وذلك بسبب معارضته للفساد الذي يسود أنشطة صندوق كلينتون، فضلًا عن سبل تعامل الحزب مع منافس كلينتون داخل الحزب الديمقراطي في الانتخابات التمهيدية بيرني ساندرز»، مؤكدًا أنه تسلم بنفسه حزمة من هذه الوثائق في سبتمبر الماضي .

الــــفصل الثانـــي:

الصراع الدولي الأمريكي
و سلاح الانترنت

الفصل الثاني: الصراع الدولي الأمريكي و سلاح الأنترنت

المبحث الأول: الصراع على الهيمنة بين (الولايات المتحدة الأمريكية – وروسيا)

هذه الحروب الإلكترونية التي بدأت تنتشر بشكل رهيب و مختلف حول العالم، شأنها لا يختلف عن الحروب التقليدية بل و أضرارها و عواقبها وخيمة، فهي تستهدف المواقع الأمنية و المصرفية و الصحية، مما يشكل خطرا على الأمن الدولي و الاقتصاد العام. تكون كيفية إيقافها بخلق جدار دفاع يمكنه صد الهجمات السيبرانية و حماية البلدان، إلا أن هذه الحلول ليست كافية، وذلك ما أثبت عند اختراق روسيا للموقع الحكومي الأمريكي، فيما يخص الإنتخابات الرئاسية الأخيرة، مما أدى إلى زعزعة الرأي العام الأمريكي و التشكيك في أساليب حماية الدولة، ولأن هذه الحروب الإفتراضية أصبحت مكشوفة فقد كشف وزير الدفاع الروسي سيرغي شويغو (Sergui Choigou) و الذي أعلن عنه في موقع Huffpost، في 22 فبراير 2017، أن روسيا أنشأت جيشا إلكترونيا تابعا لوزارة الدفاع، كما صرح الرئيس السابق بجهاز المخابرات الإسرائيلية " ناتيف "ياكوف كيدمي" ان هذا الصنف من القوات موجود في جميع الجيوش الرئيسية بما في ذلك الجيش الإسرائيلي و كذلك الأمريكي و البريطاني و الصيني.[1]

1– الصراع على الهيمنة بين الولايات المتحدة الأمريكية و وروسيا :

هذا النوع من الصراع (الهيمنة) بين القطبين الأمريكي و الروسي يتمثل في العديد من المجالات منها الفكري و العسكري و لكن هذا الصراع لم يتوقف عند الأمثلة التقليدية و إنما أصبح على شكل هجومات إلكترونية، فلم تتمكن روسيا و الولايات المتحدة من التوصل إلى تفاهم مشترك في (دبلوماسيتهما) الثنائية حول معظم جوانب الأمن السيبراني على الرغم من إعلان عام 1998 من إهتمامهم بالقيادة المشتركة للاستجابات العالمية لتحديات الأمن السيبراني، إلا أن البلدين تصرفوا في أكثر الأحيان مثل الأعداء الذين يحرسون أسرار الأمن القومي الحساسة، وليس كحلفاء ملتزمين بحماية المصالح المشتركة في الإقتصاد الرقمي العالمي و العالم المتصل بالشبكات الاجتماعية.[2]

---

[1] ايهاب خليفة، **القوة الالكترونية...كيف يمكن ان تدير الدول شؤونها في عصر الانترنت**، القاهرة: العربي للنشر و التوزيع،ط1، 2017.

[2]

و لعل أبرز ظهور لتأثير الجيوش الإلكترونية هو قيام الروس بالتدخل في الإنتخابات الأمريكية الأخيرة و الذي يكشف جانبا من هذه الحروب الحقيقية و الدافع من هذه الظاهرة الأخيرة هو تبين قوة روسيا و هدفها في الوصول هي الأخيرة إلى الهيمنة العالمية و تنافسها مع نظيرتها الأمريكية.

و بالرغم من تواجد جيش إلكتروني قوي في الولايات المتحدة، و اعتمادها على ما تسميها (الوحدات الست (The Six Units) لقيادة " الفضاء الإلكتروني "، وهي المختصة بالتخطيط و التنسيق و إدارة عمليات الحروب الإلكترونية مع باقي الفروع التي تتبعها .

وحدة الجيش الإلكتروني الأمريكي تابعة للوحدة الأمريكية لقيادة الجيش الإلكتروني و تتلقى أوامرها منها، و تتكون من ثلاثة وحدات أصغر، كذلك هناك وحدة السايبر تحت قيادة المارينز و التي تختص بحماية و تأمين منشأت المارينز من الهجمات الإلكترونية .

أما الوحدة الخامسة فهي القوة الجوية 24 و تختص بالطيران و القوات الجوية الأمريكية و يتفرع منها ثلاثة (03) أجنحة، و الوحدة السادسة هي الأسطول العاشر الأمريكي و الذي يقوم بهجمات التخابر لصالح البحرية الأمريكية، وأنشئ لغرض التنسيق بين القوات البحرية الأمريكية في الحرب العالمية الثانية، ومن أهم ضحايا الهجمات الأمريكية و أشهرها فكانت على كوريا الشمالية التي إنقطعت فيها خدمات الأنترنت تماما ليوم كامل ردا على إختراقات شركة سوني (Sony) ديسمبر 2014 و الذي سنتحدث عنه في المبحث الثاني.

أما روسيا فهي تنفي اختراقها للمواقع الحكومية الأمريكية، رغم امتلاكها أبرز و أقوى جيش إلكتروني : مخابرات الإشارة الروسية. على غرار إنكار موسكو فيما يخص ملاحقة روسيا الاتهامات بشن حروب إلكترونية على خصومها، إلا أن موقع بيزنس انسايدر (Business Insider) يؤكد أن هاكر أو مخترقين روسيين شنوا حربا على أوكرانيا بالتزامن مع عمليات إنفصال القرم .

نفس الشيء تكرر مع أوسيتيا الجنوبية " فهي جمهورية مستقلة معترف بها الا من طرف روسيا ", اذ يرى الصحفي الروسي اندريه سولداتوف أن مجموعة من المخترقين (Hacker) يعملون لصالح إستخبارات الإشارة الروسية.

كما أنهم بحسب موقع "CNN " فهم قاموا بإختراق وزارة الخارجية الأمريكية و أيضا أنظمة البيت الأبيض لدرجة تسريب جدول أعمال الرئيس الأمريكي باراك أوباما.

و هنالك سوابق تاريخية مقنعة تشير إلى أن التحفظات في روسيا و الولايات المتحدة المتأصلة في حساسية الأمن القومي يمكن التغلب عليها، على سبيل المثال، في التحضير لـ " Y2K "[1] كان هناك تهديد عالمي محتمل و تعاونت معظم الدول على الرغم من حساسيات الأمن القومي، أما روسيا و الولايات المتحدة فقد تبنيتا إجراءات متطرفة للغاية من أجل الرصيد المشترك لأكثر إجراءات الاطلاق الحساسة و التحذير من القذائف الباليستيكية.

و في الأونة الأخيرة وافقت الولايات المتحدة الأمريكية و روسيا على ترتيبات تشفير مشتركة جديدة لل " Hot Line " (الخط الأحمر) البالغ من العمر أربعين عاما بين الكرملين (Kermlin) و البيت الأبيض – علاوة على ذلك فإن البنوك الأمريكية و الروسية تتعاون مسبقا في الإتصالات الرقمية الآمنة للتحويلات الدولية للمبالغ الضخمة من الأموال .

تتعامل الولايات المتحدة الأمريكية و روسيا مع مشكلة الأمن السيبراني من زاويتين مختلفتين :

– تركز الولايات المتحدة الأمريكية على نهج تطبيق القانون على المستوى المحلي بالتعاون الدولي الطوعي.

بينما تركز روسيا على تطوير أنظمة دولية ملزمة، هناك أيضا فلسفات مختلفة تماما في العمل: روسيا تفضل السيطرة الإجتماعية على الانترنت كوسيلة، في حين أن الولايات المتحدة في معظمها، لا تفعل ذلك.

و على الرغم من هذه الإختلافات و افقت الولايات المتحدة و روسيا في ديسمبر 2009 في إجتماع للجنة الأمم المتحدة المعنية بنزع السلاح و الأمن الدولي على بدء محادثات حول تعزيز أمن الانترنت و الحد من الإستخدام العسكري للفضاء السيبراني بعد رفض روسيا لمبادرات الأمن السيبراني للعديد من السنوات، قررت الولايات المتحدة إجراء تغيير رئيسي في السياسة، في إعلانها عن أهداف الأمن السيبراني في 29 مايو 2009، أظهرت إدارة أوباما عزمها على رفع قضية الأمن السيبراني إلى مستوى جديد، وبالتالي قد تكون الإتفاقات الجديد بين الولايات المتحدة و روسيا في متناول اليد.

العا لم اليوم يواجه خطرا واضحا في العا لم الرقمي، إن المعلومات الواردة من المصادر المصنفة على مقياس و نطاق هذه التهديدات تثير قلقا أكبر بكثير من السجل العام الذي يزعج بالفعل .

[1] James A. Lewis et al, Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cyber security for the 44th Presidency, Washington, D.C., CSIS, December 2008,

في إعلانه عن سياسة جديدة للأمن السيبراني في 29 مايو 2009، أظهر الرئيس أوباما مدى تخلف و تصاعد دفاعاتها، وقال " نحن لسنا مستعدين كما ينبغي أن نكون " و أيضا إننا أخفقنا في الإستثمار في أمن البنية التحتية الرقمية (Infrastructure)لدينا"[1]. في تقرير ديسمبر 2008، لجنة نظمها مركز الدراسات الإستراتيجية و الدولية (CSIS) في واشنطن تحت عنوان " الحرب السيبرانية : المعركة الخفية" مشابهة لتلك الموجودة في الإشارات الإستخباراتية في الحرب العالمية الثانية، إستنتجت اللجنة أن " فشل أمريكا في حماية الفضاء السيبراني هو أحد أكثر مشاكل الأمن القومي إلحاحا "[2] .

في عام 2000، وقع الرئيس فلاديمير بوتين على " مبدأ أمن المعلومات"، و الذي خلص، في جملة أمور، ما يلي:

- هناك وضع متدهور مع " أمن البيانات التي تشكل أسرار الدولة".
- أكثر المتخصصين المؤهلين قد تركوا المجال في روسيا.
- تأخر تكنولوجيا المعلومات الوطنية " يجبر الحكومة على شراء معدات أجنبية، مما تزيد من إحتمال النفوذ الغير المصرح به.
- يتزايد إعتماد روسيا على شركات الكمبيوتر و الأجهزة الأجنبية السلكية و اللاسلكية .
- زيادة التهديدات باستخدام " سلاح المعلومات ضد روسيا "
- هناك " عدم كفاية التنسيق و سوء تمويل الميزانية" عندما يتعلق الأمر بالاستجابة الوطنية لهذه التهديدات .
- عدم إيلاء الإهتمام الكافي لتطوير نظم الاستطلاع الفضائي و الحرب الإلكترونية[3].

لحماية شبكات البيانات و المعلومات، تبنت الولايات المتحدة و روسيا، بالاضافة إلى بلدان أخرى، ما يشبه إستراتيجيات الحصن، مؤكدين على الدفاعات المادية. هذا النهج أكثر جدارة في العصور الوسطى على غرار زمن الأنترنت، ولكنه مفهوم، روسيا و الولايات الأمريكية لا تزالان في حشد كبير من جهود جمع المعلومات الإستخباراتية ضد بعضهما البعض، كل منها تريد إخفاء تطوير تكنولوجيا الأسلحة عن الأخرى، و كلاهما أيضا بادرتا بإجراء عمليات سيبرانية هجومية ضد بعضهما البعض، يجب النظر إلى الأمن السيبراني على أنه دفاع جيد.

[1] “President Obama’s Remarks on Securing U.S. Cyber Infrastructure,” May 29, 2009, http://www.america.gov/st/texttrans-english/2009/May/2009
[2] James A. Lewis et al, Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, Washington, D.C., CSIS, December 2008, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf . csis-prod.s3.amazonaws.com
[3] Russian Federation, Information Security Doctrine of the Russian Federation, September 2000, http://www.mid.ru/ns-osndoc.nsf/1e5f0de28fe77fdcc3

المبحث الثاني: تجربة القرصنة الروسية و الكورية (نموذجا Sony)

1- القرصنة الروسية :

لطالما أثبتت روسيا قوة سيطرتها و جدارتها سواء في الحروب التقليدية أو الحديثة و التي تتمثل في شن هجومات سيبرانية، اخرها إختراق المواقع الحكومية الأمريكية و ولوجها للأنظمة الإلكترونية داخل البيت الأبيض لكن القرصنة الروسية لم تتوقف هنا و لم تبدأ في الأونة الأخيرة .

في 03 جوان 2017، نشرت صحيفة " واشنطن بوست " مقالا حول إمكانية إمتلاك الروسيين سلاحا سيبرانيا قويا: حيث أكدت أن الهاكر الروسيين قاموا بتعطيل عمل شبكات الطاقة الأمريكية مستندة إلى دراسة قامت بها شركة " Dragos " و وفقا لهذه الأخيرة، يمكن للبرمجة الضارة التي أطلق عليها المحللون تسمية " Crash Override "، أن توقف التيار الكهربائي لفترة تمتد من ساعات حتى أيام، و ذلك ما حدث لنظام الطاقة الأوكراني في عام 2016 .

نفس الصحيفة نقلت عن رئيس قسم تحليل التجسس الإلكتروني التابع لشركة " Isight " جون هولتكفيست، أن هذا الأخير يعتقد أن مجموعة " Sandworm "[1] مرتبطة مع الحكومة الروسية.

في أكتوبر 2017، نشر موقع فرانس 24 (France 24) عن تمكن روسيا من إختراق و سرقة أسرار وكالة الأمن القومي (NSA) و ذلك بالمرور على مخبر كاسبرسكي (Kaspersky Lab) .

في عام 2015، تمكنت الجواسيس السيبرانية الروسية من سرقة معلومات عن برامج ال "NSA " و ذلك لقرصنة أجهزة الكمبيوتر و من أهداف أجنبية، محاولة التعرف على كيفية عملها، وأيضا من أجل الحصول على وسائل الدفاع التي يستعملونها ضد محاولات التسلل العدائي، إن كثير الحرب هذا سيسمح لروسيا بأن تكون على رأس أولويات جواسيس الولايات المتحدة في الفضاء السيبراني.

---

[1] اياد قاسم،"واشنطن بوست": الهاكرز الروس يملكون سلاحا سيبرانيا قويا، مقال منشور على الأنترنت (مصدر)تاريخ الدخول: 2018/03/24 https://ar.rt.com/ixn5

استولى عملاء روس على هذه الثروة من المعلومات الحساسة من خلال قرصنة الكمبيوتر المحمول لأحد المتعاقدين من الباطن من وكالة الأمن القومي الذي أخذ معه الوثائق المستهدفة، و بحسب ما ورد، فإن الوكالة الأمريكية إكتشفت هذا الإختراق في أوائل عام 2016.

أما صحيفة وال ستريت (Wall Street Journal) ، ووسائل الإعلام الأخرى، يشيرون إلى إمكانية التعاون بين شركة الأمن Kaspersky و أجهزة الإستخبارات الروسية (FSB) ، أو إختراق شركة " Kaspersky " من قبل جواسيس الكرملين، وذلك يترك " Une Faille Dans L'antivirus " ليتمكنوا بعد ذلك بإختراقها بسهولة، ولكن شركة Kaspersky Lab نفت معلومة تعاونها مع الكرملين.

قرصنة روسيا لوكالة نظم المعلومات التابعة لوزارة الدفاع الأمريكية (DISA)

وكالة نظم المعلومات التابعة لوزارة الدفاع الأمريكية Defense Information Systems Agency – DISA, تعمل بمثابة منظومة الاتصالات ونظم المعلومات الخاصة بوزارة الدفاع و تقوم بتجميع البيانات الهامة والحساسة من مصادر مختلفة لهدف واحد، هو توفير الدعم للقوة العسكرية الأمريكية في صورة متخذي القرار بدأ من الرئيس الأمريكي، مرورا بمستشاريه ووزير الدفاع حتى الجنود في ساحة المعركة.

لكي تقوم هذه الوكالة بعملها من تجميع هذا الكم الهائل من البيانات وتقديمة بشكل مناسب لكل الجهات السابق ذكرها، فإنهم بالطبع يحتاجون لمشاريع برمجية عملاقة لكي تقوم بتجميع البيانات بشكل أوتوماتيكي من كل المصادر المتاحة ثم تقوم عن طريق الذكاء الاصطناعي أو عن طريق برمجيات معدة مسبقا من استخراج المعلومات المهمة وتقديمها للجهات المعنية السابق ذكرها.

بالطبع مشاريع بهذا الحجم لا يمكن لوزارة الدفاع الأمريكية بكل مشغولياتها من توفير فرق متخصصة لبرمجة هذه المشاريع، لذلك يعتمد الجيش الأمريكي على شركات خارجية متخصصة في برمجة مثل هذه الأنظمة وهذه الشركات تعمل فقط لصالحة وزارة الدفاع الأمريكية في برمجة أنظمة الاتصالات العسكرية.[1]

أحد هذه الشركات والتي يملكها John C. Kingsley قامت في العام 2010 بتوظيف مبرمجين روسيين للعمل لديها في برمجة عدة برامج خاصة بوكالة نظم المعلومات التابعة لوزارة الدفاع الأمريكية، وبالفعل تم

---

[1] ابراهيم حجازي، **كيف إستطاعت المخابرات الروسية إختراق وزارة الدفاع الأمريكية منذ عام 2008**، مقال منشور على الانترنت (مصدر) تاريخ الدخول: 2018/03/02

https://www.security4arabs.com/2015/11/29/how-the-russians-hacked-disa/

صدور البرامج المطلوبة وتم تنصيبها داخل ما يسمي بالشبكات الآمنة والتي يفترض أنها تحتوي على السيرفرات(الخوادم) التي تحمل البيانات السرية التابعة للوكالة دون علمهم بما تحويه هذه البرمجيات من برمجيات خبيثة أخري لا حصر لها، حتى أن Patrick Malone وصف الأمر ب أوكازيون الفيروسات Viruses occasion.وبهذه الطريقة استطاع الروس الوصول إلي قلب وزارة الدفاع الأمريكية بكل ما تحويه أنظمتهم من أسرار واتصالات على مدار الساعة.

تم اكتشاف برمجيات خبيثة تعمل داخل الشبكات الحساسة التابعة للوكالة، تم التكتم على الأمر حتى عمل الفحوصات اللازمة للشبكات والأجهزة العاملة بالوكالة. كانت نتيجة البحث أن اختراق هذه الأنظمة تم عن طريق البرمجيات التي قامت ببرمجتها شركة Net Cracker في ذلك المشروع من العام 2008 وشركات أخري ساهمت في هذا المشروع في أوقات لاحقة، فقامت الوكالة برفع قضية ضد كل الشركات التي ساهمت بالعمل في هذا المشروع وتم تقديم مدراء الشركات للمحاكمة. و هذه القضية دامت في المحاكم الأمريكية طيلة أربع سنوات متواصلة إلي أن تم الحكم فيها في شهر نوفمبر من هذا العام 2015 .

مجمل أحداث القضية كانت كالتالي:

1- Computer Sciences Corporation والمتورطة أيضا في هذه القضية باستئجار مبرمجين روسيين للعمل لديها، تقاضت مبلغ وقدره واحد ونصف مليار دولار من وزارة الدفاع الأمريكية نظير المشاريع البرمجية التي تقدمها لوزارة الدفاع ووكالة ال DISA

2- المبرمجين الروسيين اللذين عملوا لدي الشركات المتورطة في هذه القضية قد شاركوا في كتابة برامج دخلت حيز الخدمة في:

وكالة نظم المعلومات التابعة لوزارة الدفاع الأمريكية DISA, سلاح الطيران الأمريكي وإدارة الخدمات العامة (General Services Administration)

3- على مدار أربع سنوات من المحاكمة وتقديم الادعاءات والأدلة ونفيها، لم يستطع محامو الجهات المتضررة من إلحاق تهمة الخيانة أو التورط بالجاسوسية إلى أي من أصحاب الشركات المتورطة في هذه العملية، وتم الاتفاق على التعويض حيث ستقوم الشركات المتورطة بدفع مبالغ مالية للجهات المتضررة كتعويض عن الخسائر التي لحقت بشبكاتها والبنية التحتية التي تضررت من جراء تلك الاختراقات.[1]

[1] ابراهيم حجازي، <u>نفس المرجع السابق</u>

أشارت بعض التقارير إلى أن هذه الموجة من الهجمات الإلكترونية "على مستوى عالمي" تثير قلق خبراء أمن المعلومات ، الذين لفتوا إلى أن القراصنة قد يكونون استفادوا من ثغرة أمنية في أنظمة "ويندوز"، كشفت النقاب عنها وثائق سرية خاصة بوكالة الأمن القومي الأميركية تمت قرصنتها .من بين الدول التي تم اختراق أنظمتها المعلوماتية كل من بريطانيا وروسيا وأوكرانيا والهند والصين وإيطاليا وإسبانيا وأستراليا وبلجيكا وفرنسا وألمانيا والمكسيك ومصر، فيما اعتبرت أسوأ موجة هجمات متزامنة في التاريخ.

ومن بين المؤسسات والشركات التي تعرّضت أنظمتها الالكترونية للهجوم منظومة الرعاية الصحية الوطنية في بريطانيا والسكك الحديدية في ألمانيا وشركة "تيليفونيكا" الإسبانية للاتصالات و"إيرباص" وغيرها .وفي روسيا تم استهداف أنظمة وزارة الداخلية والطوارئ والصحة ومصرف "سبيربنك" وشركة "ميغافون" للاتصالات. ويقوم البرنامج الخبيث المستخدم في الهجمات بإغلاق ملفات المستخدمين، ويجبرهم على دفع فديات مالية مقابل إعادة فتحها. وكانت السلطات الأميركية حذرت يوم الجمعة من موجة الهجمات المتزامنة، مناشدة ضحاياها عدم دفع أموال للقراصنة.

إلى ذلك، اشارت صحيفة (دايلي تلغراف) اللندنية إن البرمجية الخبيثة، التي يعتقد أنها استخدمت في موجة الهجمات الأخيرة، لجأت إليها للمرة الأولى مجموعة هاكرز "Shadow Brokers" عقب الضربات الأميركية على سوريا، ما يفسره بعض الخبراء بتواطؤ روسي مع المجموعة .وذكرت "تلغراف" أن Shadow Brokers أدانت الاعتداء الأميركي على سوريا، وفي اليوم التالي وجّهت "تحذيرًا" إلى الرئيس الأميركي دونالد ترامب. وبعد أسبوع، شنّت المجموعة هجومًا إلكترونيًا باستخدام برمجيات خبيثة، قالت إنها سرقتها من وكالة الأمن القومي الأميركية.

أما رئيسة الوزراء البريطانية تيريزا ماي، قالت إن الهجمات الإلكترونية على مستشفيات المملكة المتحدة هي جزء من هجمة دولية كبرى .من جهته، ذكر موقع "ويكيليكس" أنه كان قد حذر سابقًا من انتشار غير منضبط للبرمجيات الخبيثة من قبل الاستخبارات الأميركية، وذلك في سلسلة نشراته ."Vault 7" وكان الموقع نشر في 7 مارس 2016، أكبر عملية تسريب لوثائق سرية من وكالة الاستخبارات المركزية الأميركية تحت مسمى "Vault 7"". وكما يشير موقع(Politico) ، وهو البرنامج الذي أنتجته وكالة الأمن القومي الأميركية، يسمح للبرمجيات الخبيثة بالانتشار عبر بروتوكولات تبادل الملفات المثبتة على أجهزة حواسيب كثيرة من المؤسسات حول العالم .وأكد Politico أن الهاكر في هذه الهجمات يستخدمون البرامج التي استخدمتها وكالة الأمن القومي الأميركية على شكل واسع، وفقًا لتغريدة العميل السابق للوكالة، إدوارد سنودن.

القرصنة الكورية :

شهدت مؤخرا الولايات المتحدة و كوريا الشمالية أزمة كبيرة تسببت في الكثير من القلق للعالم بسبب تجارب بيونغ يانغ النووية، لكن ليس هذا فقط، فكوريا الشمالية تمتلك أيضا احدى أهم و أقوى الجيوش الإلكترونية الذي يمتد إلى 6 ألاف قرصان موجودين في كافة أنحاء العالم، مهمتهم سرقة ملايين الدولارات و الهجوم على شركات و إدارات عامة.

ذكرت صحيفة نيويورك تايمز أن الجيش الإلكتروني الكوري حاول في عام 2016 سرقة مليار دولار من الاحتياطي الفيدارالي بولاية نيويروك، لكن أجهزة الإنذار رصدت العملية نتيجة الخطأ في الكتابة، وفي شهر ماي 2017، نفذت الجواسيس السيبرانية الكورية الخاصة بالرئيس " كيم جونغ أون " عمليات ضد آلاف أجهزة الحاسوب في عدة دول و جمدوا شبكة هيئة الصحة البريطانية لمدة ساعات بإستخدام فيروس الفدية " Ransom ware" " وانا كراي" " Wannacry" .

و من بين أبرز العمليات التي قاموا بها هجومهم على شركة الإنتاج الفني " Sony Picture Entertainment "، وذلك لسببين: أولهم منع عرض لفيلم الكوميدي السياسي "The Interview " (المقابلة) لأنه يسخر من الرئيس الكوري " كيم جونغ " و من نظامه السياسي الإشتراكي "، و ثانيا كان هدفهم الرد على قرصنة أمريكا للبرامج الإلكترونية الخاصة بكوريا الشمالية في عام 2010 و ذلك ما أكدته صحيفة " Le Quotidien " حيث نقلت معلومات عن مسؤولين أمريكيين و أجانب طلبوا عدم الكشف عن هويتهم بالإضافة إلى وثيقة و كالة الأمن القومي خبر قرصنة كوريا عبر الشبكات و الإتصالات الصينية و الماليزية و التي يفضلها الهاكرز بكوريا الشمالية .كان الهدف من وراء هذا الإختراق جمع معلومات حول البرنامج النووي للنظام الكوري.

بعد خمسة أشهر من فضيحة قرصنة شركة " Sony " ، أصدرت و يكليكس 30287 وثيقة من أرشيف مجموعة Sony، مع إمكانية إجراء عمليات بحث سهلة .

و في بيان، أعلن موقع ويكليكس 132173 بريدا إلكترونيا من و إلى أكثر من 2200 عنوان SPE، و التي قال محرر و يكليكس أنها تندرج تحت " المجال العام " و التي تمكننا الأن البحث عن طريق الإسم أو كلمة مفتاحية.

من بين تلك الوثائق المسربة التابعة لشركة "Sony" ، صور الرئيس التنفيذي مايكل لينتون (Michael Lynton) يتناول العشاء مع الرئيس الأمريكي أوباما، و موظفين يجمعون الأموال للديمقراطيين، بما في ذلك حاكم نيويورك أندرو كومو (Andreau Cuomo) .

" تعرف شركة "Sony" بتقدمها و إنتاجها للأفلام و الترفيه، لكن ما تبينه السجلات أن " وراء الكواليس هذه الشركة الترفيهية هي في الحقيقة شركة مؤثرة، حيث لها علاقات مع البيت الأبيض (هناك ما يقارب 100 عنوان إلكتروني من حكومة الولايات المتحدة في هذه الأرشيفات)، مع القدرة على التأثير على القوانين و السياسة، وكذلك فهذه المعلومات المسربة عن "Sony" كشفت روابط مع المجمع العسكري الصناعي الأمريكي

(**Le Complexe Militaro-Industrielle**)

قد يكون هذا سببا أخر ضمن الأسباب التي دفعت بكوريا الشمالية لقرصنة هذه الشركة و التي قالت عنها الـ (FBI) أنها من بين أخطر عمليات القرصنة .

و قد تم بالفعل وضع هذه البيانات على الأنترنت في نوفمبر من العام الماضي 2017، بعد أن كانت شركة (SPE)، وهي شركة تابعة لمجموعة "Sony" اليابانية، ضحية لعملية قرصنة هائلة، وقد سرقت البيانات الشخصية لــ 47000 موظف و أطرف ثالثة بما في ذلك المشاهير، بالإضافة إلى وثائق مالية و مخطوطات، ورسائل بريد إلكتروني و غيرها. نشر بعضها بشكل غير قانوني، بالإضافة إلى خمسة أفلام من الأستوديو.

ذكرت صحيفة نيويورك تايمز أن بيونغ بانغ تسعى إلى إظهار قدرتها أمام العالم بعيدا عن التهديد النووي، كما أنها تستغل القرصنة كمصدر للتمويل وتعتبر البنوك أهدافا أساسية بالنسبة لها في عملياتها غير القانونية.

و أضافت هذه الصحيفة أن قراصنة كوريا الشمالية اخترقوا بنوك في الفلبين و بنغلادش و فيتنام كما أنهم إخترقوا أنظمة معلوماتية في بنوك مركزية بـ المكسيك و فنزويلا و البرازيل، و في ماي 2017، ضرب فيروس " وان كراي " (Wanna Cry)، الذي صممه قراصنة كيم، 300 ألف حاسوب في كبرى الشركات متعددة الجنسيات، اذ يعمل الفيروس على حجب المعلومات المخزنة على الجهاز و من ثم يطلب دفع فدية للسماح للمستخدم بالوصول مرة أخرى إلى بياناته المسجلة .

تعتبر هذه التقنية توجها جديدا على نظام بيونغ يونغ، اذ عمد الرئيس الحالي منذ توليه السلطة في 2011، إلى تعزيز إستخدام التكنولوجيا من أجل الاضرار بأعداءه و من بينهم الولايات المتحدة الأمريكية و كوريا الجنوبية.

و قد صرح رئيس قسم أبحاث كوريا في " مركز الدراسات الإستراتجية " بواشنطن " فيكتور شا " بأن :

" عمليات القرصنة السيبرانية توسعت بشكل كبير ضمن الإستراتيجية القومية التي تتبعها كوريا الشمالية، وخلال فترات السلام تسمح للبلد الأسيوي بالاختراق دون التعرض للعقوبة أو القمع، وفي أوقات الحرب سوف تقوم العمليات بالإطلاع على خطط الولايات المتحدة و كوريا الجنوبية لإضعاف جيوشها."

ووفقا لــ " نيويورك تايمز" فإن كثير من قراصنة كيم " تلقوا تدريبا في الصين و الولايات المتحدة، و حتى الان لايزال الرد ضعيفا على هجمات نظام "كيم " الإلكترونية، اذ ان التهديد النووي استنفذ كل تركيز العالم، ولم تسهم العقوبات التي فرضتها الولايات المتحدة في ردع بيونغ يانغ.

و يرى الخبراء أن الهجوم السيبراني هو الطريق المثلى بالنسبة لنظام بيونغ يانغ، لأنه يدرك أنه لن تستطيع أي دولة الرد عليه عسكريا، ولكن رغم وجود قراصنة كيم في عدة دول فإن أجهزة المخابرات تحاول رصدهم باستخدام إجراءات تتبع للكشف عن الخلايا الإرهابية .

المبحث الثالث: القرصنة الروسية في الإنتخابات الرئاسية الأمريكية

رغم نفي روسيا للإتهامات التي وجهت إليها فيما يخص قرصنة الإنتخابات الرئاسية الأمريكية الأخيرة، إلا أنه قد روسيا قد قامت بالفعل بإختراق مواقع و أنظمة حكومية لدول مستهدفة لذلك لا يمكن إستبعاد هذه الإتهامات بشكل مطلق .

و تذهب بعض التقارير الأمريكية إلى أن موسكو نفذت من كل عملية إختراق خوادم (Server) حواسيب اللجنة الوطنية للحزب الديمقراطي الأمريكي، عملية إستخباراتية كبرى سعت من خلالها إلى تسهيل وصول " مرشحها دونالد ترامب إلى البيت الأبيض، ضمن إحدى حولات الصراع المتجدد مع واشنطن، ورغم المبالغات الممكنة في هذا الأمر الذي تغذيه وسائل الإعلام الأمريكية، فإن موسكو وفق التقارير الرسيمة الأمريكية و التحقيقات الجارية هدفت إلى زعزعة أركان الديمقراطية الأمريكية و إحداث حالة من الفوضى السياسية تثير الشكوك في مدى تماسك النظام السياسي الأمريكي .

نتجت عن هذه القرصنة السيبرانية طرد الرئيس باراك أوباما لـ 35 دبلوماسيين روس قبل مغادرته البيت الأبيض، وكان ذلك كرد على مزاعم الإختراق الروسي الذي تنفيه موسكو دائما.

وفي إحدى التقارير التي نشرتها صحيفة " نيويورك تايمز " يؤكد مسؤولون في الإستخبارات الأمريكية أن تحرك القراصنة الروس في أنظمة حواسيب الحزب الديمقراطي نؤاجل لعدة أشهر، وشملت عدة مسؤولين بالحزب بما في ذلك هيلاري كلينتون و إعتبرت هذه المبادرة الغير القانونية في مجال الحروب الإلكترونية و الإرهاب السيبراني الذي إتفقت عنه لجنة الأمم المتحدة على أنه في فئة الجرائم اذ يهدد أمن و إستقرار الدول .

أما عن هذه القضية، فقد نشرت التفاصيل في موقع و يكيليكس، مما أدى بصحيفة التايمز البريطانية بنشر تقرير بدور موضوعية حول أسانج، رئيس تحرير موقع ويكليكس و ادوارد سنودن، الموظف السابق في جهاز المخابرات الأمريكية، وتظن هذه الصحيفة أن الهدف من وراء التسريبات هو شن حرب إلكترونية، وأيضا لإحداث تغيرات سياسية في الأسباب الحاكمة بالولايات المتحدة و أوروبا.

توضح صحيفة " نيويورك تايمز " أن الموظف الإستخباراتي السابق " سنودن " قد قام لشكف برامج المخابرات الأمريكية و البريطانية في التجسس على المواطنين و القيادات بالدول الغربية الحليفة، أما صاحب موقع ويكليكس الاسترالي "أسانج" فقد قام بنشر الرسائل المقرصنة من الحزب الديمقراطي، مما يطرح الكثير من الأسئلة حول علاقتها بموسكو قبل و بعد إستقرارهما فيها.

و تؤكد بعض النظريات أن الإستخبارات الروسية نفذت عملية الإختراق و سربت الوثائق لاحقا لأنساج في مستقرة بسافرة الإكوادور في لندن .

ذكرت صحيفة ' وول ستريت " يوم الخميس أن وزارة العدل الأمريكية جمعت أدلة كافية لمفاضات ستة من أعضاء الحكومة الروسية : المتورطين في إختراق اللجنة الوطنية للحزب الديمقراطي (DNC) قبل الإنتخابات الرئاسية لعام 2016، لكن الإعتقلات أو الأحكام بالسجن قد تكون غير محتملة ووفقا لصحيفة " Le Quotidien "، فإن الوكلاء الفدرالين و المدعين العامين من واشنطن و فيلادلفيا و بيترسبرغ و سان فرانسيسكو تعاونو في التحقيق لرفع القضية إلى المحكمة في العام التي تلي الإنتخابات، ولكن من خلال تحديد المسؤولين عن القرصنة، يمكن أن تجعل سلطات الولايات المتحدة سفرهم إلى الخارج أكثر تعقيدا لكن كما أكد سابقا فمن غير المحتمل أن تكون هناك إعتقالا أو حكم بالسجن .

و بعد أن نشرت بعض الصحف الأمريكية أن هذه القرصنة الروسية التي إستهدفت الإنتخابات الرئاسية لتكون في صالح دونالد ترامب، فهذا الأخير ينفي تماما هذا الخبر، ذلك مما دفع بلجان البرلمان لفتح عدة تحقيقات في ما يخص بدخل روسيا المفترضة في هذه الإنتخابات خاصة بعد نشر رسائل البريد الإلكتروني و الوثائق الحكومية من قبل ويكليكيس في 2016 لكن ترامب تحلى قرارا النتائج التي توصلت إليها و كالات الإستخبارات الفيدرالية بأن روسيا لها دخل في إختراق الحزب الديمقراطي لمصلحة المرشح الجمهوري .

و من جهة أخرى، تنشر صحيفة "The Nation '

الأمريكية مقالة تعلق فيه عن هذه الت تقضي عن الشائعات التي تدور حول المجتمع الأمريكي و " Ruissiangate " و تتناول المقالة موضوع إستحالة قرصنة نظام اللجنة الوطنية الديمقراطية (CND) في 05 جويلية من عام 2016، حيث تقول أنه لم تكن هناك أي قرصنى لا من قبل الروسي و لا من قبل أي شخص أخر.

و تستدل بدليل " علمي قوي" أن هذه الظاهرة قد تكون تسربا، أو تنزيلا تم تنفيذه محليا بإستخدام مفتاح

USB أو أي جهاز محمول أخر للتخزين البيانات، و أضافت " The Nation " أن هذه الظاهرة

عبارة عن ما يسمى بـ " وظيفة داخلية ' أو "Coup Monté " Inside Job

من قبل شخص لديه قدرات للوصول إلى نظام الكمبيوتر الخاص بـ CND، وما يبعث إلى تشكيك

بهذه " القرصنة " الأولية، التي من المفترض أنها أدت إلى نشر عدد كبير من الوثائق من ويكليكس، وثانيا تقر الصحيفة أنه ليس هناك أدلة كافية لإدانة موسكو وإتهامها، و ذلك لأن التقارير الناتجة من وكالة الإستخبارات الأمريكية تفترض و لاتؤكد.

لاحقا و في نفس الصحيفة، معلومات حول الفاعل الرئيسي وراء هذه " القرصنة"، فتظهر مراجعة قضائية للوثائق التي تم نشرها قبل أسبوعين من قبل شخص أو كيان معروف تحت إسم Guccifer 2.0، وكانت إحتيالية، تقول الصحيفة أن قبل أن تضع Guccifer هذه الوثائق على الأنترنت، تم تزويرها، وبمعنى أخر، تم قص و لصق هذه الوثائق في قالب مستند فارغ تميز بلغة إفتراضية روسية. و في 15 جوان 2017، أقرت مجموعة Guccifer أنها كانت المسؤولة وراء هذا التدخل في نظام CND، صرح هذا التدخل في 14 جوان 2017، و أعلن " كمصدر ويكليكس، و هو أمر ضروري لمصداقية الحساب الرسمي الذي يشمل روسيا في ما كان سيصبح "عملية قرصنة على نطاق واسع "، ولكن الفحص العلمي الفضائي لم يأخد هذه الحكاية، وذلك لأسباب جد مقنعة حيث أن الضربات الأولى للمجرمين، التي نشرت في الصحيفة في 9 جويلية، تتعلق بكمية الأجهزة التي كان من المفترض إختراقها و ما يعرف بإسم " معدل النقل " Taux de Transfert، أي مقدار الوقت الذي يستغرقه الإختراق، التحليل الذي يمكن تقديمه هو حساب المسافة و الوقت و المقدار، فقد أجريت العملية من مسافة بعيدة (روسيا)، أما البيانات الوصفية فقد دونت عددا من الحقائق حول هذا الأمر بدقة كبيرة: في مساء 5 جويلية 2016، تم تنزيل 1.976 ميجابايت "MB من البيانات من خادم CND، وإستغرقت العملية 87 ثانية، وهذا ما يعطي معدل نقل 22.7 ميجابايت Mb في الثانية.

هذه الإحصائيات ذات طبع عام وضرورية لفحص (نفي) نظرية القرصنة، فطبقا لهذه الإحصائيات تبين أنه لا يتمكن أي مزود خدمة أنترنت، من أولئك الذي لجأ إليهم الهاكر في منتصف 2016، من تنزيل البيانات بهذه السرعة، مما خلق تناقض كبير، حيث أن Guccifer إدعى أنه قام بعملية القرصنة من رومانيا، و لأسباب عديدة من الناحية التقنية تسمى Delivery Overheads، إضطرت لإبطاء سرعة القرصنة من خلال الإبتعاد عن السرعة القصوى الممكنة.

وبذلك نطرح السؤال التالي: ما هي السرعة القصوى الممكنة ؟ أجرت مؤخرا Forenicaror إختبار عن طريق تحميل ما يعادل حجم البيانات (وبإستخدام سرعة نقل لم تكن متاحة في 2016) على

مسافة 40 ميلا من جهاز الكمبيوتر الخاص بهم، من خلال خادم و الذي يتواجد على بعد 20 ميل

وكان قادرا على تحقيق سرعة التحميل 11.8 ميغابايت في الثانية أي نصف ما كانت عملية قرصنة CND بالحاجة إليه لو إفترضنا أنها كانت قرصنة قام محققون آخرون بنعطيل و بقراءة دقيقة لهذه الظاهرة، أما فولدن (Folden) و ادوارد لوميس(Edward loomis) استشهدوا بدراسة نشرت في 3 اوت 2016 من قبل www.speedtes.net/reports، و الذي هو موثوق للغاية و يستعملونه في سجلاتهم، و تشير هذه الدراسة إلى أن أكبر سرعة ISP (مزودي خدمة الأنترنت) كات مستهلكة من قبل الشركتين ' XFinity ' و ' Cox ' للإتصالات في منتصف 2016، و تراوحت هذه السرعة من 15.6 ميغابايت في الثانية إلى 14.7 ميغابايت في الثانية، كما أنه تم ملاحظة قيم سرعة عليا بشكل متقطع، لكنها لم تصل بعد إلى 22.7 ميغابايت في الثانية.

يقول Folden: " لا يمكن أن تتحقق سرعة 22.7 ميغابايت، خاصة اذا كنا نتحدث عن نقل البيانات عبر المحيطات "، ويضيف : " اذا اعتمدنا على البيانات المتضمنة فان ما يسمى بالقرصنة أمر مستحيل "

أما " Forenscator " فقد أعلنت عامة عن إختبار السرعة أجرته مؤخرا، هذا الإختبار يعزز إلى حد كبير هذه الإستنتاجات: معدل نقل 23 ميغابايت / ثانية (Gb/s) ليس مستبعدا إلى حد كبير، ولكن من المستحيل تحقيقه عند توصيل بيانات الأنترنت من مسافات معتبرة '...'.

بالإضافة إلى ذلك، يتم قياس سرعة النسخ المحلية، وهذه القياسات تظهر أن 23 ميجابايت في الثانية هو معدل نقل نموذجي عند إستخدام مفتاح « Usb Flash » .

و في ظل هذه المعلومات المتناقضة يمكننا فهم فرضيات تعتبر فيها قضية تدخل روسيا في الإنتخابات الرئاسية الأمريكية معتبرين موقع ويكيليكس و ما أداه الموظف السابق للإستخبارات الأمريكية و البريطانية إدوارد سنودن، وكذلك قضية Guccifer و تحليل Forensicator و Folden و نستنتج إحتمال أن روسيا اخترقت خادم الحزب الديمقراطي بدافع مساعدة ترامب ليصل إلى الرئاسية و رغم الأدلة الكاقية من كل الطرفين (المعارضين و المؤيدين لقضية القرصنة) إلا أن الرئيس الروسي " فلاديمير بوتين " ينفي أي تدخل، وكذلك ترامب الذي ينفي بدوره إمكانية قرصنة روسيا لـ DNC، ولكن رغم ذلك فالأدلة لم تكن أبدا كافية ضد روسيا،

فإما أنه هناك عميل مزدوج (أو عملاء) في الحكومة الأمريكية، أو إحتمالية تواجد عيوب في النظام الحكومي، أما بالنسبة لقضية هيلاري و كلينتون و مشكلة تسريب رسائلها الإلكترونية، فقد تكون بعامل داخلي لكنها تمسكت بحتمية تدخل روسيا بهدف تخريب حملتها الإنتخابية و تشويه سمعتها و سمعة الحزب الديمقراطي لصالح دونالد ترامب، حيث أن جون بوديست (John Podesta) يتهم تعامل ترامب مع الروسيين، وذلك لأن و كالة الإستخبارات الأمريكية (CIA) تؤكد أنه تم اختراق نظامها الداخلي.

في حين أن الحزب الجمهوري لم يدلي بأي مشاكل مع القرصنة و لم تتواجد أي تسريبات فيما يخص مع القرصنة و لم تتواجد أي تسريبات فيما يخص حملته، ثم قضية Guccifer المزعومة و التي إتضحت أنها مجرد كذبة و هذا ما أثبته forensicator و Folden .

الفصل الثالث

مشكلات وعيوب القرصنة و علاقتها بالعمل الإستخباراتي

الفصل الثالث: مشكلات و عيوب القرصنة و علاقتها بالعمل الإستخباراتي

المبحث الأول: نقد القرصنة الروسية و الإستخبارات الأمريكية

اتسمت نهاية القرن العشرين بثورة تكنولوجية و معلوماتية هائلة، أحدثت قفزة غيرت أنماط الحياة و حدود العلاقات، امتدت من فضاء الاتصالات إلى المصارف و الأنظمة المالية، إلى التجارة و التسويق و التسوق، إلى التعليم و التكوين، إلى تسيير المواصلات و المطارات و القطارات، إلى إدارة المنشآت العسكرية و النووية، إلى فضاءات التواصل الاجتماعي، وحتى إنشاء الحكومات الإلكترونية.

أنتج هذا التعامل مع الانترنت و ما توفره من زخم معلوماتي و قدرات اتصال و خدمات، حالة من الارتباط، يصعب على الفرد و المؤسسات الاستغناء عنها، أين أضحت الإنترنت جزء من الحياة اليومية للأشخاص و الهيئات، كما أفرز هذا التعامل و هذا الارتباط كمًا هائلا من البيانات و المعلومات، تباينت في طبيعتها بين العام و الشخصي، العلني و السري. برزت ظواهر سلبية في التعامل مع هذه الشبكة، أبانت إضرارا بمصالح الأشخاص و الهيئات و الدول عن طريق الاختراق و القرصنة، الأمر الذي طرح مسألة التعامل الآمن و حماية المعلومات.

إزداد التعامل مع الفضاء المعلوماتي يوما بعد يوم حتى بلغ مستويات تعد قياسية. حيث يورد تقرير البنك الدولي لسنة 2016، و الموسوم بـ " تقرير عن التنمية في العالم 2016 : العوائد الرقمية " عدة أرقام تدل على أهمية و تطور الخدمات الرقمية ، حيث يشير إلى أنه يتم ارسال 207مليار رسالة رقمية يوميا، و مشاهدة 8.8مليار فيديو على اليوتوب في اليوم، و 803مليون تغريدة يوميا، و 152مليون مكالمة عبر سكايب، وإجراء 4.2مليار عملية بحث على غوغل.

أفرز هذا التعامل الكثيف في الفضاء الشبكي و حجم الخدمات المتوفرة فيه تزايدا لجرائم المعلوماتية و لحجم الأضرار و النفقات المترتبة على إصلاحها، وكذا تكاليف العمل على تأمينها و حمايتها ، حيث يشير التقرير السنوي للشركة الأمريكية سيمونتيك المختصة في أمن المعلومات لسنة 2016، أن عدد الجرائم المعلوماتية قد زاد بنسبة 10 بالمائة عن سنة 2015 ، و أن عدد ضحايا الجرائم المعلوماتية في فضاء الانترنت لسنة 2015 بلغ 689 مليون شخص، موزعين على 21 دولة و أن حجم الأضرار تجاوز 126 مليار دولار لسنة 2015 لوحدها.

تَعْرِف القوة المعلوماتية إهتماما متسارعا من طرف الدول ، فبقدر ما تسعى الدول لإمتلاك التكنولوجيا و التحكم في استخداماتها و توفير خدمات الاتصالات اللازمة، بقدر ما تتخوف من تهديدات الاختراق و التجسس. يعتبر المنظر الاستراتيجي الأمريكي جوزيف ناي (Joseph Nye) في مقال له بعنوان "مستقبل القوة" "The Future of power" نشر سنة 2011، أن القوة المعلوماتية والتي يختزلها في القوة السيبرانية، أنها ستكون محور العلاقات الدولية في المرحلة القادمة ، و سيكون امتلاكها حاسما في إدارة العلاقات الدولية تشهد جرائم المعلوماتية ازدهارا كبيرا في روسيا التي تشكل مقرا لعمليات قرصنة وتجسس كبرى استهدفت جهات منتشرة في مختلف أنحاء العالم، وسط اتهامات للسلطات في موسكو بالتقاعس عن اتخاذ التدابير الرادعة اللازمة للقضاء على هذه الشبكات[1].

ارتبط تصاعد الصراع بين روسيا والدول الغربية بقيادة الولايات المتحدة، خلال السنوات الماضية، باستدعاءٍ متنامٍ لحرب المعلومات Information Warfare كأحد المداخل الهامة للتأثير في مسارات الصراع. ففي خضم التنافس على قيادة النظام ؛ تَشَكَّلَ توجُّهٌ استراتيجي مغاير لدى موسكو، له امتداداته التاريخية في الحقبة السوفيتية.

هذا التوجه مفاده أن الانتصار في الصراع مع الغرب لن يتحقق بالاعتماد القاصر على الأدوات العسكرية التقليدية، ولكن الأمر يتطلب تفعيل أدوات الحرب المعلوماتية وغيرها من الأدوات غير التقليدية، وهو ما أطلق عليه رئيس هيئة الأركان العامة الروسية "فاليري جيراسيموف" نهجًا مختلفًا لتحقيق الأهداف السياسية والعسكرية الروسية من خلال "الطرق غير المباشرة وغير المتماثلة."

صدرت في عام 2012 وثيقة وزارة الدفاع الروسية المعنونة "مفهوم الأنشطة الفضائية للمعلوماتية للقوات المسلحة بالاتحاد الروسي 'The Russian Federation Armed Forces " Information Space Activities Concept، لتكشف عن الحيز الهام الذي تمثله المعلومات في الإطار الاستراتيجي الروسي، وتبنت الوثيقة تعريف فضاء المعلومات بأنه "مجال النشاط المتصل بتشكيل المعلومات ونقلها واستخدامها وتخزينها، مما يؤثر على الوعي الفردي والمجتمعي، فضلًا عن المعلومات في معناها الضيق، وكذلك الهياكل الأساسية للمعلومات."

في عام 2013، نشر الجنرال الروسي رئيس هيئة الأركان العامة الروسية "فاليري جيراسيموف" مقالًا عن التحديات الجديدة وأساليب تنفيذ العمليات القتالية، وكان هذا المقال بمثابة تأسيس لما يُعرف في الغرب بـ"عقيدة جيراسيموف"The Gerasimov doctrine ، وهذه العقيدة تنطوي على مجموعة من الأفكار بشأن الأدوات غير التقليدية في الحروب الراهنة، والتي تتضمن أدوات مختلفة من بينها المعلومات، سواء من خلال الفضاء الإعلامي أو الفضاء الإلكتروني، واستهداف نقاط الضعف للخصوم، وتجنب المواجهة العلنية حتى المراحل النهائية للصراع.

[1] Joseph S. Nye Jr. **The Future of power**. Public Affairs New York, État de New York , 2011.

لقد كان "جيراسيموف" يُعبّر عن أطروحةٍ تَزَايَدَ استحضارها في روسيا خلال السنوات الماضية، مع سعي موسكو الحثيث لاستعادة إرثها التقليدي كقوة مؤثرة في النظام الدولي، وما يستلزمه ذلك من توظيف أدوات الحرب المعلوماتية. وفي هذا السياق، اعتمدت روسيا في ديسمبر ٢٠١٦ وثيقة "عقيدة أمن المعلومات في الاتحاد الروسي " Doctrine of Information Security of the Russian Federation، وأكدت الوثيقة البُعدَ العسكري لمسألة المعلومات كأساس لأمن الدولة، وتُحدد "أسلحة المعلومات" باعتبارها إحدى الأدوات لتحقيق الأهداف السياسية.

وكان من شأن هذه الأطروحات شرعنة استخدام مجموعة واسعة من الأنشطة والعمليات التي تسعى إلى التلاعب أو تشويه أو سرقة أو خلق أو تدمير المعلومات وإعادة إنتاج الروايات المضللة لخدمة المصالح الروسية، أو بمعنى آخر فإن هذه الأنشطة والأدوات غير المتناظرة تجاوز أو –على أقل تقدير– تحيد القدرات الغربية العسكرية، وتستغل الثغرات في المجتمعات الغربية.[1]

يعتقد ديفيد سميث David J. Smith في دراسة له بعنوان "كيف تستخدم روسيا الحرب السيبرانية؟"، أن روسيا "تعتمد على مفهوم واسع للحرب المعلوماتية، يشمل: الاستخبارات، والتجسس المضاد، والخداع، والتضليل، والحرب الإلكترونية، وتدمير الاتصالات وأنظمة دعم الملاحة، والضغوط النفسية، بالإضافة إلى الدعاية وإلحاق الضرر بنظم المعلومات ."

ووفقًا لهذه الرؤية تبدو الحرب المعلوماتية الروسية مستندة بشكل جوهري إلى أداتين رئيسيتين:

1- التضليل المعلوماتي

ينبني هذا المدخل على كيفية توظيف الأدوات الإعلامية والدعائية المختلفة بهدف إعادة إنتاج روايات مضللة للآخرين، ومشوهة للحقائق، تُضعف روايات الأطراف الغربية المناوئة، وتخدم في نهاية المطاف المصالح الروسية. وقد تجلّى هذا النمط أثناء تعاطي وسائل الإعلام الروسية مع الأحداث السياسية التي شهدتها الدول الغربية. لقد تحدثت العديد من التقارير الغربية عن حملات تضليل مارستها روسيا أثناء الانتخابات الرئاسية الأمريكية في عام 2016 من خلال وسائل الإعلام الروسية، وفي مقدمتها شبكة تليفزيون "روسيا اليوم"، حيث سعت الشبكة إلى تشويه صورة المرشحة الديمقراطية "هيلاري كلينتون"، واتهامها بالفساد، والعلاقة مع المتطرفين الإسلاميين، ناهيك عن التركيز على الرسائل الإلكترونية التي تم تسريبها للمرشحة، وتنفي موسكو تلك الاتهامات. وتكرر هذا النموذج في الانتخابات الرئاسية الفرنسية في عام 2017؛ إذ منعت حملةُ الرئيس الفرنسي "إيمانويل ماكرون"، المحسوب على تيار الوسط، ممثلي شبكة تليفزيون "روسيا اليوم" ووكالة "سبوتنيك" الروسية من الدخول إلى مقراته، وبرر المتحدث باسم الحملة هذا المنع "بتعمد كلا الجهتين إصدار أخبار وهمية ومعلومات كاذبة للإضرار بماكرون."

---

[1] Mark Galeotti, « The Gerasimov Doctrine and Russian Non-Linear War », blog In Moscow's Shadows. Analysis and Assessment of Russian Crime and Security, mis en ligne le 6 juillet 2014.

2- القرصنة الإلكترونية

يُشكِّل الهجوم على البنية المعلوماتية للدول الأخرى جزءًا هامًّا من استراتيجية حرب المعلومات الروسية، باعتباره وسيلة للحد من فعالية الخصم، وإرباكه وتضليله، ناهيك عن فعالية عمليات القرصنة في تجزئة نظام القيادة لدى القوى المناوئة لموسكو، والسيطرة عليها ولو حتى لفترة زمنية محدودة.

وعلى الرغم من نفي موسكو تورطها في عمليات القرصنة الإلكترونية التي تعرضت لها الدول الغربية خلال السنوات الماضية؛ إلا أن هذه الدول كثيرًا ما كانت تؤكد التورط الروسي في هذا الشأن، لا سيما مع طبيعة الدول التي تعرضت لعمليات القرصنة والعلاقات التي تجمعها بروسيا، ناهيك عن الجماعات التي أعلنت ارتكابها عمليات القرصنة التي كانت في الغالب تحمل الجنسية الروسية[1].

ففي عام 2007، تعرضت أستونيا لهجمات قرصنة إلكترونية استهدفت عددًا من المؤسسات الحكومية والبنوك ووسائل الإعلام، وبدا من طبيعة الأحداث وسياقها الزمني تورط روسيا في الهجمات؛ إذ إن الهجمات تزامنت مع توتر في العلاقات بين روسيا وأستونيا عقب قرار الأخيرة إزالة نُصب تذكاري يعود للحقبة السوفيتية من العاصمة الأستونية تالين.

وقد تم استدعاء القرصنة الإلكترونية بصورة أكثر كثافة إبان الحرب الروسية الجورجية، وفي 7 أغسطس 2008 بينما كانت وحدات الجيش الروسي تعبر الحدود إلى جورجيا، اتهمت روسيا بشن هجوم سيبراني على مواقع الحكومة ووسائل الإعلام والمنظمات المالية والتجارية وغيرها في جورجيا.

وفيما كانت الدول الغربية تكثف من انتقاداتها واتهاماتها لروسيا، كانت موسكو تنكر التورط في عمليات القرصنة الإلكترونية، وفي الوقت ذاته كانت تصوغ نموذجًا جديدًا من العلاقات، يطلق عليه "تيم مور " Tim Maurerتوظيف وكلاء سيبرانيينCyber Proxy Actors ، من منظمات ومجموعات للقرصنة تخدم مصالحها، وتسمح لها بالتنصل من الاتهامات الغربية.

ولعل أبرز هذه المجموعات مجموعة APT28 الروسية التي اتهمتها ألمانيا باختراق بيانات لنواب في البرلمان الألماني في عام 2015، واستخدام برامج خبيثة لمهاجمة العديد من الأجهزة المستخدمة من قبل النواب والموظفين. وفي العام ذاته هاجمت المجموعة قناة "تي في 5 موند" الفرنسية، وهو ما أدى إلى إيقاف بث القناة لساعات، والإضرار بأنظمتها.

وتمتلك مجموعة APT29 هي الأخرى قدرات وموارد متقدمة ومتطورة، دفع الكثيرين من المحللين الغربيين إلى افتراض وجود علاقة بينها وبين النظام الروسي، فضلًا عن استهداف المجموعة الكيانات للاستيلاء على المعلومات التي ترتبط ارتباطًا وثيقًا بالمصالح الجيوسياسية الروسية. وخلال السنوات الأخيرة ازداد تركيز المجموعة على أهداف استخباراتية متصلة بالصراع في أوكرانيا، وهو ما يتضمن مجموعة واسعة من المؤسسات الغربية، مثل: الحكومات، والأجهزة الأمنية، ومراكز الفكر والرأي.

---

[1] نوران شفيق، **أثر التهديدات الألكترونية على العلاقات الدولية دراسة في أبعاد الأمن الألكتروني**، المكتب العربي للمعارف، القاهرة، 2018 .

وتُقدم مجموعة Cyber Berkut نموذجًا آخر لمجموعات القرصنة الموالية لروسيا، وارتبط بزوغ المجموعة بتطورات الصراع داخل أوكرانيا، حيث تتبنى المجموعة خطابًا معاديًا للغرب، ومواليًا لموسكو بشكل أو بآخر. وقد نفذت المجموعة عددًا من الهجمات داخل أوكرانيا لعل أهمها في مايو 2014 حينما أعلنت مسئوليتها عن اختراق أنظمة لجنة الانتخابات المركزية الأوكرانية في الانتخابات البرلمانية على النحو الذي عطل أنظمة فرز الأصوات.

يفترض "بافل أنتونوفيتش Pavel Antonovich" أن "ترسيم الخطوط الفاصلة بين الحرب والسلام يمكن أن يتآكل بسهولة في الفضاء السيبراني، فيمكن أن يتم إلحاق أضرار، مهما كانت طبيعتها، بالخصم، وذلك دون تجاوز الخط الفاصل بين الحرب والسلام بشكل رسمي."

وما ذهب إليه "أنتونوفيتش" يكشف عن المكاسب التي تحققها حرب المعلومات لموسكو، فبينما تتحقق المصالح الروسية، لن يكون على روسيا الانخراط في صراعات مباشرة مع القوى الغربية، وكبديل عن ذلك يتم استخدام المعلومات في الصراع دون أن تتحمل موسكو تكاليف الحرب المباشرة، ناهيك عن افتقار الفضاء المعلوماتي لقوانين تضبط سياسات الدول ومواقفها إزاء بعضها بعضًا [1] .

وبوجه عام تتمثل أهم الدوافع لمقاربة حرب المعلومات الروسية فيما يلي:

أولًا– خلق بيئة متسامحة :Permissive environment إذ إن حرب المعلومات تستهدف خلق بيئة متسامحة تجاه المصالح والرؤية الروسية، ولا يتوقف إيجاد مثل هذه البيئة على إدراج المعلومات التضليلية في سلسلة صنع السياسات على سبيل الحصر، ولكنه يمكن أن يجري عبر وسائل الإعلام الجماهيري والاجتماعية لإحداث تأثير في آراء وتوجهات الأفراد العاديين، ومن ثم جعلهم أكثر تقبلًا وتسامحًا مع الرواية الروسية الرسمية، وبالتالي تخفيف حدة المقاومة لسياسات موسكو. ولا يُمكن إغفال أن بزوغ قوى اليمين المتطرف في أكثر من دولة غربية يسهم في تدعيم هذا الهدف الروسي، لما لهذه القوى من علاقات تعاون مع موسكو.

ثانيًا– تقويض القدرة على المواجهة: فالكثير من عمليات حرب المعلومات الروسية، وخاصة فيما يتعلق بالقرصنة الإلكترونية، تُضعف من إمكانات خصوم موسكو وقدرتهم على المواجهة، وهو ما تجلى بشكل كبير في الحرب الروسية الجورجية 2008، حيث إن الهجمات السيبرانية التي نُفذت في جورجيا بالتزامن مع دخول القوات الروسية أفضت إلى تعطيل استجابة جورجيا للغزو الروسي، لا سيما مع ما أدت إليه عمليات القرصنة الروسية من إضعاف قنوات التواصل بين الحكومة والجمهور، وإيقاف المعاملات المالية، بالإضافة إلى عرقلة انتقال المعلومات حول ما يحدث في مناطق الحرب إلى العالم الخارجي.

ثالثًا– تشويه القوى المناهضة: ووفقًا لهذا الطرح وظّفت روسيا المعلومات لتشكيل سرديات وروايات تشوه القوى المناهضة لها، وفي الوقت ذاته تشييد صور إيجابية لحلفائها، فقد ظلت روسيا لسنوات تروج لمقولات أن الثورات الملونة التي شهدتها جورجيا وأوكرانيا كانت نتاجًا لمجموعات من المحرضين المدعومين من الولايات المتحدة كجزء من التدخل الخارجي المتعمد في كلا الدولتين من أجل إخراجهما من المدار الروسي.

---

[1] Douglas Lovelace,**The Cyber Threat**, Oxford University Press,nov. 2015 – 376 p

وقد استحضرت روسيا هذا النموذج أثناء الانتخابات التي شهدتها الدول الغربية في السنوات الأخيرة حينما وقفت بجانب تكتلات ومرشحين محسوبين على تيار اليمين المتطرف (على غرار مارين لوبان في فرنسا، أو حتى الرئيس الأمريكي دونالد ترامب)، وتشويه صورة القوى المنافسة عبر توظيف الأدوات الدعائية والقرصنة الإلكترونية.

رابعًا– إثارة المشكلات الداخلية: حيث تنطوي حرب المعلومات الروسية على التكريس لأوضاع داخلية مأزومة في المجتمعات الغربية، فحينما أثار الإعلام الروسي قضية الفتاة الألمانية (من أصل روسي) ليزا في عام 2016 التي ادّعت أنه تم الاعتداء عليها من قبل رجال لهم ملامح شرق أوسطية، كان يحاول الضغط على الحكومة الألمانية عبر استدعاء قضية اللاجئين بما تتضمنه من دلالات سلبية ضاغطة في الكثير من المجتمعات الغربية[1].

وعلى الرغم من تكشُّف اختلاق هذه الرواية من جانب الفتاة الألمانية، فقد كانت بمثابة تعبير عن توجه روسي للضغط على الغرب بملف اللاجئين، وليس أدل على ذلك من تصريحات وزير الخارجية الروسي "سيرجي لافروف" على خلفية القضية": نتمنى لألمانيا وهي قاطرة الاتحاد الأوروبي كل النجاح في مواجهة المشكلات الهائلة مع المهاجرين، وألا تُخفي تلك المشكلات تحت السجادة، وألا تتكرر حادثة ابنتنا ليزا."

ومن جهةٍ أخرى، فإن عمليات القرصنة الإلكترونية تُحدِث خسائر فادحة في المجتمعات الغربية، خاصةً مع التوجه نحو مهاجمة البنية التحتية في هذه المجتمعات مثلما حدث في أوكرانيا في ديسمبر 2015 حينما تم احتراق شبكة الكهرباء في المنطقة الغربية إيفانو فرانكوفسك، وهو ما أدى إلى إيقاف عمل الشبكة وانقطاع الكهرباء في المنطقة.

خامسًا– مواجهة العقوبات الغربية: فعقب تدخل روسيا في أوكرانيا عام 2014، وضم شبه جزيرة القرم بعد استفتاء مارس 2014، تزايدت العزلة الأوروبية المفروضة على روسيا، واعتمدت الدول الأوروبية آلية للعقوبات ضد روسيا في مارس 2014 تتضمن عددًا من الإجراءات، كحظر التأشيرات، وتجميد الأصول، وفرض قيود تجارية واقتصادية. كما تزايدت العقوبات الأمريكية المفروضة على روسيا .

وفي هذا الصدد، مثَّلت حرب المعلومات أحد مسارات الاستجابة الروسية لهذه العزلة لما يمكن أن تلحقه من خسائر بالمجتمعات الغربية، ولذا فإن أحد التفسيرات التي طُرحت لعملية القرصنة التي تعرض لها الحزب الديمقراطي أثناء الانتخابات الرئاسية الأمريكية عام 2016 كانت تصوير القرصنة على أنها ثأر من الحزب الذي وسَّع حزمة العقوبات الاقتصادية المفروضة على روسيا .

وفي إطار تلك الحرب، وُجهت اتهامات لروسيا باستخدام وسائل التواصل الاجتماعي للترويج لأخبار كاذبة كان لها تأثير كبير في نتائج الانتخابات الرئاسية الأمريكية . كما تحمل التطورات التكنولوجية المتلاحقة إيجابيات عدة في مجال التنمية والتطور ودفع قاطرة التقدم للأمام، إلا أنها في نفس الوقت تحمل بين ثناياها مخاطر

---

[1] ستيفن لي مايرز، **القيصر الجديد**،(ترجمه:تيسير نظمي خليل) (المملكة العربية السعودية-الرياض : نشر و توزيع: العبيكان،ط1، 2018)، ص 369.

مقلقة، لا تهدد حياة الفرد والمؤسسات فحسب، بل تعرض الأمن القومي للدول والشعوب للخطر أيضًا، وهو ما كشفته التقارير الواردة في هذا الشأن.

من الأهمية بمكان الإشارة إلى أن مصطلح »حروب الجيل الرابع» يطلق على حروب غير تقليدية، كما كان يتم في الجيل الأول من الحروب والذي استمر لقرون، و«الجيل الثاني» كأسلوب الحرب الباردة التي انتهجتها الولايات المتحدة لتفكيك الاتحاد السوفياتي، ثم بدأ «الجيل الثالث» تحت اسم الحرب على الإرهاب، وهو السبيل الذي انتهجته الولايات المتحدة لمحاربة أعدائها، ولكن بعدما أدركت أن تكلفة هذا النوع من الحروب ضد جماعات الإرهاب، أضحت باهظة على المستويات البشرية والمادية على حد سواء، سيما بعدما عانت من خسائر كبرى في الحروب التي شنتها في الميدانين الأفغاني، والعراقي، ومن قبلهما كينيا، وتنزانيا، والصومال، فكان «الجيل الرابع» القائم على فكرة «التدمير الذاتي» لأعداء الولايات المتحدة[1].

ويستخدم في هذه الحروب ما يعرف بحرب المعلومات، وتعتمد على شقين: الأول دفاعي يحمي أنظمة الدولة، والثاني هجومي يوجهه ضد أنظمة الدولة المعادية، وتستخدم في هذه الحرب العمليات النفسية، عبر أجهزة الاستخبارات، وتشمل مهاجمة الوسائط، والهاكرز، وأعمال التجسس، وزرع العملاء إلى أن يتكون مناخ عدائي بين الأطراف الداخلية ومؤسسات الدولة ونسيجها الوطني فيبدأ الصراع الداخلي. وثمة تقديرات تشير، في هذا السياق، إلى أن صعود حروب الجيل الرابع ارتبط بالتغير في توازنات القوى الدولية، على النحو الذي لم يعد يخول لواشنطن فعل ما تبتغيه، من دون معارضة دولية متعددة المستويات، في ظل صعود أدوار الاتحاد الأوروبي، والصين، وعودة روسيا للاضطلاع بأدوار رئيسية على الساحة الدولية.

تسعى الولايات المتحدة الأمريكية إلى تبني إجراءات احترازية، وتدابير وقائية قبل حلول موعد الانتخابات الرئاسية عام 2020. ورغم ذلك، ثمة الكثير من التحديات، التي يرتبط بعضها بحجم المواقع الإلكترونية وأعداد متابعيها، حيث هناك نحو 328مليون مستخدم على «تويتر»، وما يقرب من مليارى مستخدم في «فيسبوك»، بما يزيد من تعقيد المهمة، ويجعل أية قدرة على النفاذ، وتغير الأكونتات أمراً في غالب الأحيان مرجحا، ويصعب التعاطي معه، على نحو سريع.

وفي هذا السياق، يشير سكوت شانيسبت، إلى أنه على الرغم من أن «تويتر «و«فسيبوك» كانتا بطيئتين نسبيا في التصدي لمشكلة التلاعب، فقد كثفتا جهودهما لمتابعة «الحسابات المزورة»، حيث قام «فيسبوك» بإزالة نحو مليون حساب يومياً، بما في ذلك بعض تلك التي كانت تتعلق بالانتخابات الفرنسية والألمانية الأخيرتين.

وقد تركزت الأنظار أخيراً على شركة «كاسبرسكي للأمن المعلوماتي» بعد معلومات عن استخدام قراصنة روس أدواتها لسرقة أسرار وكالة الأمن القومي الأميركية، في خضم النزاع المحتدم في الفضاء الرقمي بين الولايات المتحدة وروسيا. وصدرت أوامر أخيرا بإزالة برمجيات «كاسبرسكي لابز» من أجهزة الكومبيوتر في جميع الوكالات

[1] د.فيصل محمد عبد الغفار، **الحرب الإلكترونية**، الإمارات العربية المتحدة، 2016.

الأميركية. من جهتها، أكدت الشركة عدم ارتباطها بأي حكومة معتبرة في بيان أصدرته أنها ببساطة «علقت في وسط معركة جيوسياسية». ولفتت الاتهامات الأخيرة الأنظار إلى ما وصفه البعض بـ«حرب معلوماتية» دائرة بين القوتين الأميركية والروسية. وأشار، بيتر سينجر، الذي ألف كتباً حول أساليب الحرب في القرن الـ21، إلى أن روسيا متقدمة في هذا »الصراع المعلوماتي».

وقال سينجر: «إن كانت حربا معلوماتية فهي أشبه بالحرب الباردة في كل شيء، من سرقة الأسرار إلى عمليات التأثير واختراق الجبهة الداخلية». وأوضح» :نظراً إلى أن الروس نجوا حتى الآن من أي تبعات فعلية لعمليتهم الأضخم والأكثر تأثيراً، أي الاختراقات وحملة التأثير على انتخابات 2016، فبرأيي أنهم يبدون أداء جيداً جداً.«

وفي هذا الصدد، قال جيمس، الباحث في مركز الدراسات الاستراتيجية والدولية، إن روسيا متقدمة على هذا الصعيد، لأنها «أدركت كيف تستخدم حرياتنا المدنية ضدنا ولا يمكننا فعل الكثير بهذا الشأن». وأضاف: «ليست لدينا مجموعة تمارس هذا النوع من الحرب النفسية ولا نملك السلطة القانونية للدفاع عن أنفسنا أمامها .« في المقابل، اعتبر، غبريال وايمان، أستاذ الأمن المعلوماتي في جامعة حيفا بإسرائيل أنه قد يكون من السابق لأوانه إعلان فوز روسيا. وقال: «نجهل حقيقة إنجازات وكالة الأمن القومي الأميركية في مراقبة الإنترنت، فهذا النوع من المعلومات سري». وأضاف: «إنها لعبة القط والفأر، ترد فيها جهة على الاختراق وتبادلها الجهة الأخرى بالمثل، فتزداد خطورة وتعقيداً.

لا شك أن اتهامات أجهزة الاستخبارات الأمريكية لروسيا ولرئيسها شخصياً بالتورط في عمليات قرصنة إلكترونية استهدفت الحملة الديمقراطية للانتخابات الرئاسية، تنطوي على مسائل بالغة الخطورة بالنسبة للأمن القومي للدول، ناهيك عن أن تكون مرتبطة بدولة عظمى كالولايات المتحدة والأمن الدولي بصفة عامة.

من أبرز الأسماء التي سقطت فريسة للقرصنة الإلكترونية ، وزيرة الخارجية الأمريكية السابقة ومرشحة الرئاسة الخاسرة هيلاري كلينتون، والتي كشفت أجهزة الاستخبارات الأمريكية تعرض المرشحة الديمقراطية لعمليات قرصنة وتجسس على بريدها الإلكتروني الخاص من قبل جهات روسية.

وقد أشارت كبريات الصحف في أمريكا إلى تورط أجهزة مخابرات روسية في التجسس على هيلاري لصالح المرشح الجمهوري دونالد ترامب، حيث مررت الوثائق التي حصلت عليها بشأن الحزب الديمقراطي إلى موقع ويكيليكس الذي قام بدوره بنشرها، مما تسبب في تشويه صورتها وإضعاف موقفها، ومن ثم الخسارة أمام منافسها، وهو ما دفع الرئيس الأمريكي باراك أوباما إلى فتح تحقيق موسع في سلسلة من الهجمات الإلكترونية خلال موسم الانتخابات الأمريكية[1].

[1] فيصل محمد عبد الغفار، **نفس المرجع السابق**

يعد الرئيس الأمريكي دونالد ترامب (Donald Trump) من أكثر الرؤساء الأمريكان إثارة للجدل عبر التاريخ الأمريكي سواء من حيث سيرته الشخصية ، وتصرفاته ، وتصريحاته ومواقفه العنصرية تجاه العرب والمسلمين والأفارقة ، وأخيراً فوزه في الانتخابات الرئاسية ، هذا الفوز الذي فاجئ الجميع وخالف كل التوقعات . فعندما أعلن ترامب ترشحه للسباق الرئاسي لم يأخذه الكثيرون على محمل الجد واعتبروا هذا الإعلان نوع من المزاح الثقيل أو المراهقة السياسية والتصرفات الصبيانية على اعتبار أن فرصه في الفوز ضعيفة جداً أو شبه معدومة ، لكنه حقق المفاجأة وفاز أولاً بثقة الحزب الجمهوري ليكون مرشحه في الانتخابات ، ثم حقق المفاجأة الأكبر والأشد وقعاً عندما تمكن من الفوز على المرشحة الديمقراطية والسياسية العتيدة والدبلوماسية المخضرمة هيلاري كلينتون ، ليتم تنصيبه الرئيس الخامس والأربعون للجمهورية الأمريكية وسط ذهول ودهشة الكثير من السياسيين والمراقبين والمهتمين بالشأن السياسي وحتى الناس العاديين في داخل الولايات المتحدة الأمريكية وخارجها. .

ومنذ اليوم الأول لتسلمه منصب الرئاسة كثرت حوله الشائعات والأقاويل والتأويلات والتسريبات والشكوك طالت كل مفاصل حياته ، إلا أن أهم وأخطر هذه الأقاويل والشكوك كانت تلك المتعلقة بفوزه في الانتخابات ، وبشكلٍ أدق ، التشكيك في نزاهة تلك الانتخابات والحديث عن وجود تدخل قوى أجنبية فيها والمقصود هنا روسيا

لم تبق الأحاديث والتشكيكات حبيسة الغرف المغلقة بل خرجت إلى العلن وتناولتها الصحافة الأمريكية ، وتم التركيز عليها في وسائل الإعلام المتنوعة ، وأصبح كل يوم يمر يزيد حجم وتعقيد هذه القضية التي صارت مثل كرة الثلج كلما تدحرجت أكثر كلما زاد حجمها ، الأمر الذي أثار قلق العديد من الأطراف في الكونغرس وفي الحكومة الأمريكية ودفعهم إلى فتح تحقيق أو تحقيقات في هذه القضية

وقد تطور الموقف من هذه الاتهامات من التشكيك في صحتها إلى التسليم بها، وإن كان هذا لا يعني القبول بلا قيد ولا شرط بكل تفاصيلها، ففي البداية استخف الرئيس المنتخب بها وعلق عليها قائلا إن مصدرها هو ذاته مصدر الادعاءات التي ثبت زيفها بامتلاك العراق أسلحة دمار شامل لتبرير الغزو الأميركي له، لكن ممثلي أجهزة الاستخبارات الأميركية ثابروا على التمسك باتهاماتهم وخلال مثولهم أمام لجنة الخدمات المسلحة بمجلس الشيوخ في الخامس من يناير الجاري حذّر مدير الاستخبارات الوطنية ومدير الأمن الإلكتروني ونائب وزير الدفاع، من الدور المتنامي لروسيا في مجال القرصنة الإلكترونية والتجسس، وقال مدير الأمن الإلكتروني إن عدد الجواسيس الروس في الولايات المتحدة اليوم أكبر منه خلال الحرب الباردة، ونتيجة هذه المثابرة بدأت المواقف تتبدل من هذه

الاتهامات بدرجات مختلفة. فقد سلم بها الرئيس أوباما واتخذ قرار طرد عشرات الدبلوماسيين الروس، وقبلها آخرون دون مبالغة في تأثيرها على نتيجة الانتخابات، كما فعل رئيس مجلس النواب الذي رفض توجيه الانتقاد للرئيس المنتخب وقال إن موقفه من هذه القضية محق في ظل محاولة البعض استخدامها للتشكيك في صدقية انتخابه، وزاد بالقول إن القرصنة الروسية لم تؤثر في نتيجة الانتخابات، لكن روسيا لابد أن تُعاقب على ما ارتكبته.[1]

أذيع ملخص لتقرير أعدته أجهزة الاستخبارات الأميركية أكد أن الرئيس الروسي أمر في 2016 بشن حملة لاستهداف انتخابات الرئاسة الأميركية بهدف تقويض الإيمان الشعبي بالعملية الديمقراطية الأميركية وتشويه سمعة هيلاري كلينتون والتأثير سلباً على إمكان انتخابها للرئاسة، وذلك عن طريق اختراق رسائل بريد إلكتروني تابعة للحزب الديمقراطي بغرض إيذائها، وقال التقرير إن الوكالات الاستخبارية واثقة تماماً من أن الاستخبارات العسكرية الروسية استخدمت وسطاء من أمثال ويكيليكس لنشر هذه الرسائل الإلكترونية التي جمعتها من اللجنة الوطنية الديمقراطية ومن شخصيات بارزة في الحزب الديمقراطي.

وقد نفت روسيا هذه الاتهامات نفياً قاطعاً، وظل ترامب يرفض مزاعم القرصنة الروسية واصفاً إياها بأنها حملة سياسية من خصومه حتى اجتمع مع مدير الاستخبارات الوطنية ومدير وكالة الاستخبارات المركزية ومدير مكتب التحقيقات الفيدرالي، وعقب الاجتماع صرح بأنه يحترم العمل الذي أنجزه المجمع الاستخباراتي الأميركي والخدمة التي أسداها، دون أن يشير إلى روسيا، كما قلل –وهذا مفهوم– من تأثير عمليات القرصنة على الانتخابات، لأن القول بغير ذلك يلقي بظلال من اللاشرعية على الرئيس نفسه، أصبح من السهل جدا اختراق الحسابات الشخصية لدى العاملين فى الاستخبارات الوطنية الأمريكية، بدءا من جيميس كلابر، مدير الاستخبارات الوطنية الأمريكية، الذى تعرض للمرة الثانية لاختراق، وهذه المرة من قبل مراهق أمريكى يدعم القضية الفلسطينية، ووزير الأمن الداخلى الأمريكى جون برينان، الذى اخترق حسابه الشخصى من قبل مجموعة من قراصنة الانترنت، وهذا ما كشف فشل الاستخبارات الأمريكية فى نظام الأمن الإلكترونى لديها.

كما تعرضت الاستخبارات الأمريكية إلى هاكرز من روسيا والصين حيث أكدت شركة فاير آى الأمريكية فى الأمن الإلكترونى إن الهاكرز الروس استطاعوا الاستحواذ على أسرار عسكرية أمريكية، وتعتقد الاستخبارات الأمريكية بوجود دعم حكومى للهجمات الكمبيوترية التى كان الهاكرز يشنونها منذ عام 2007 على مواقع الناتو والشركات العاملة لحساب وزارة الدفاع الأمريكية، وهناك مشاكل أخرى تتعلق بالهاكرز الصينيين،

[1] فيصل محمد عبد الغفار، **نفس المرجع السابق**

لكن الهاكرز الروس أكثر كفاءة، ودائما تخشى الاستخبارات الأمريكية من الهاكرز الروسى أكثر من الهاكرز الصينيين،وقال كلابر فى كلمة القاها بجامعة تكساس،ولفت إلى "عدم وجود فرق عملى بين المجموعات الاجرامية للهاكرز الروس وأولئك الذين يعملون لصالح الحكومة لأن هناك تبادلا للخبرات بينهم."

وأشارت التحقيقات الأمريكية إلى أن الاختراق قد تم من خلال تسلل هاكرز مجهولين إلى حاسوب مكتب موظفى الخدمة الحكومية الأمريكى الذى يتلقى ملايين طلبات التوظف من الأمريكيين، بما فى ذلك الوظائف الدبلوماسية حيث يتولى المكتب التصديق على الموافقات الأمنية الخاصة بهم

وجهت الولايات المتحدة الأمريكية الإتهام رسميًا إلى عنصرين من الاستخبارات الروسية واثنين من القراصنة لإختراقهم موقع ياهو وتسريب وسرقة بيانات 500 مليون حساب فيها، وهذه هي المرة الأولى التي تتهم فيها الحكومة الأمريكية الجواسيس الروس في قضايا قرصنة تقنية[1].

ووجهت وزارة العدل الأمريكية 47 تهمة مختلفة منها التجسس الاقتصادي، سرقة الأسرار التجارية، الاحتيال الحاسوبي، الدخول غير المصرح به للأنظمة والأجهزة وانتحال الشخصية. وترى الولايات المتحدة أن الاستخبارات الروسية تعمل بتعاون وثيق مع قراصنة للتجسس على شركات أمريكية وزيادة نطاق قدراتهم الاستخباراتية بمقابل السماح لهم بالإستفادة ماليًا من هذه الثغرات.

وكانت ياهو قد أعلنت عندما تم اختراقها أن الهجمة التي تعرضت لها هي بتنظيم ودعم دولة أجنبية. والمثير للإهتمام أن جهاز الأمن الفيدرالي الروسي استخدم خدمات قراصنة مطلوبين للولايات المتحدة مثل Alexsey Belan الذي اعتقل في أوروبا ومن ثم هرب إلى روسيا قبل أن يتم ترحيله لأمريكا.

وورد اسم Karim Baratov الذي يحمل الجنسية الكندية وأصله من كازاخستان ضمن لائحة الإتهام أيضاً. إن عملية القرصنة التي قامت بها روسيا كانت تهدف لجمع معلومات استخباراتية، إلا أن القراصنة الذين نفذوها استخدموا العملية أيضاً لجمع معلومات تفيدهم مالياً على المستوى الشخصي.

كانت ياهو قد تعرضت لعمليتي قرصنة، الأولى في 2013 أدت إلى تسريب معلومات مليار حساب، والثانية لاحقاً تضرر منها 500 مليون حساب. وخسرت ياهوو 350 مليون دولار من قيمة صفقة الاستحواذ بعد انتشار أخبار الاختراقات

[1] فيصل محمد عبد الغفار، **نفس المرجع السابق**

وصف عضو الكونجرس الجمهوري السابق ومدير وكالة الاستخبارات الأمريكية)سي أي ايه) الحالي مايك بامبيو خدمة ويكيليكس وما تنشره من تسريبات بأنها جهاز مخابرات معادى للولايات المتحدة يشكل تهديدا للأمن القومي الأمريكي بكل ما تحمله الكلمة من معان.

و اعتبر بامبيو – في محاضرة أمام مجلس أمناء مركز الدراسات الاستراتيجية و الدولية في واشنطن – أن تسريبات ويكيليكس تهدف إلى إلحاق "دمار ذاتي" بالقيم الغربية التي تحترم "الشفافية و الخصوصية" لكنها في الوقت تمس الأمن القومي بما تحتويه من أسرار او انشطه او معلومات.

وبرغم استفادة حملة ترامب في الانتخابات الرئاسية الأخيرة و توظيفها لما سربته ويكليكس عن مدير حملة كلينتون الانتخابية السابق جون بوديستا، إلا أن البيت الأبيض هاجم تسريبات ويكيليكس لملفات تخص الأمن القومي الأمريكي وأنشطه المخابرات الأمريكية وأخرى تتناول اتصالات البريد الإلكتروني ومراسلات التواصل الاجتماعي لشخصيات عامة وسياسية[1] .

وقال مدير وكالة الاستخبارات الأمريكية إن التعامل مع ملف تهديدات ويكيليكس وصاحبها جوليان أسانج لن يكون سهلا وسيحتاج إلى وقت طويل وكذلك سيتطلب الأمر جهدا غير تقليدي من الاستخبارات الأمريكية لمنع تسييس تلك التسريبات ذات الطابع الأمني أو استخدامها في أغراض المساومة السياسية مع الولايات المتحدة.

كما تعهد بامبيو بملاحقة اسانج وأعوانه باعتبارهم تهديدا للأمن القومي الإمريكي، مشيرا إلى أن اسانج لا تغطية الحماية الدستورية التي يتمتع بها الأمريكيون لأنه ليس مواطنا أمريكيا حيث يحمل الجنسية الأسترالية.

كانت ويكليكس قد سربت في منتصف العام الجاري 8000 وثيقة تحوى أسرارا كثيرة و معلومات حساسة عن أنشطة الاستخبارات الأمريكية وما تقوم به من أنشطة استهداف تجسسي اليكترونية معقدة تعتمد على اختراق الهواتف المحمولة الذكية وشبكات الحاسب والحسابات الشخصية عبر البريد الإلكتروني بل والتسلل إلى داخل مقر السكن وغرف النوم من خلال توظيف كاميرات أجهزة التليفزيون الذكية المتصلة بالإنترنت.

وقد سبق لخدمة ويكيليكس نشر ربع مليون وثيقة سرية تحوى برقيات دبلوماسية للسفارات الأمريكية بعضها يخص أنشطة الاستخبارات والاتصالات السياسية السرية لدول كالعراق وأفغانستان وجميعها وضعت الإدارة الأمريكية وخارجيتها والبنتاجون وأجهزة الاستخبارات في حالة ارتباك واصابتها بضيق شديد.

[1] Silva, Eugenie, **National Security and Counter intelligence in the Era of Cyber Espionage**, hershey PA, USA, 2015.309p

كذلك لمح مدير الاستخبارات الأمريكية إلى استفادة الاستخبارات العسكرية الروسية من تسريبات ويكليكس التي تم الحصول عليها من خلال عملية اقتحام رقمي للجنة الوطنية للحزب الديمقراطي الأمريكي وهو ما تيقنت منه المخابرات الأمريكية وإضافة إلى ذلك استخدمت التليفزيون الروسي المملوك للدولة معلومات مستقاة من ويكليكس في برامجه السياسية باستفادة موسكو من نشاط ويكليكس سياسيا.

تجدر الإشارة في هذا الصدد إلى أن إدوارد سنودن المتعامل السابق مع المخابرات الأمريكية هو الشخص الذى سرب معلومات وقعت تحت يده تخص الأمن القومي الأمريكي ووزارة الخارجية إلى جوليان اسانج المقيم حاليا في روسيا كلاجئ سياسي وذلك بعد أن أقام أربعة أعوام متصلة بسفارة الاكوادور في لندن هربا من ملاحقة قضائية له في السويد بتهم تتعلق باعتداءات جنسية واغتصاب طلبت بموجبها السلطات السويدية تسليمه.

وقد اتهم مدير الاستخبارات الأمريكية كلاهما بالخيانة وبالبحث عن الشهرة الذاتية والارتزاق المالي من خلال الإتجار بما لديهما من مستندات سرية. وكان اسانج قد كشف عن حيازته لمستندات تثبت استثمار أجهزة الاستخبارات الأمريكية لمليارات الدولارات في تطوير برامج للمراقبة والاختراق الرقمي وبرامج فيروسية متطورة واستخدمت ذلك كسلاح في مواجهة شركات عملاقة و مؤسسات سياسية واقتصادية وهى اتهامات لم يؤكدها أو ينفيها مسؤولي الاستخبارات الأمريكية .

وفى كاليفورنيا أكدت "سيمانتيك كوربوريشن" إحدى شركات الأمان الرقمي الامريكية الرائدة أن ما وصلت اليه ويكليكس من معلومات حساسة عن انشطة الاستخبارات الأمريكية وشملت نحو 40 عملية تجسس أمريكية في 16 دولة حول العالم هي نتاج عملية قرصنة اليكترونية دولية تمت الاستفادة فيها من تداخل شبكات الحاسب والاتصالات الدولية الخاصة بالطيران والمؤسسات المالية وحركة النقد الدولية والطاقة والطيران حول العالم

تمارس الاستخبارات الامريكية أكبر عمليات تجسس بشتى الاشكال في داخل الولايات المتحدة الامريكة وخارجها حيث يمنح قانون برامج المراقبة والتجسس صلاحيات كبيرة وواسعة لوكالة الاستخبارات القومية الامريكية بالتجسس على المواطنين الامريكين بصورة اثار ضجة كبيرة في الوسط السياسي للولايات المتحدة الامريكية ومن أكبر مبرراته محاربة الارهاب.

تشير معلومات ووثائق متعددة أن وكالة الأمن القومي الأمريكي تتجسس حتى على أطراف النخبة العالمية بما في ذلك البنك الدولي وصندوق النقد الدولي والأمم المتحدة وحتى الفاتيكان. وايضا بحسب الوثائق ان الأمن القومي الأمريكي كان ولا زال يتجسس على كل سيناتور أمريكي منذ أربعين سنة على الأقل. هذا وقد اثار مرشح الرئيس الأمريكي دونالد ترامب النائب مايك بومبيو لمنصب مدير وكالة المخابرات المركزية الأمريكية مخاوف بعض المشرعين من أن ذلك التعيين قد يوسع المراقبة أو يسمح باستخدام أساليب استجواب معينة اعتبرت على نطاق واسع أساليب للتعذيب.

حيث بعد احداث 11 سبتمبر بدأت الاستخبارات الامريكية تستخدم وسائل تعسفية للمراقبة والتجسس في داخل الولايات المتحدة الامريكية وكثفت عمليات التجسس على المواطنين الامريكيين وذلك بحجة منع حدوث عمليات ارهابية من قبل متطرفين في داخل امريكا

فقد قامت الاستخبارات الامريكية بفرض رقابة وتجسس على هواتف وحواسيب مئات الملايين من المواطنين والمسؤولين في الولايات المتحدة الامريكية وذلك في ظل انتشار وتداول وسائل الاتصال الالكتروني بكثرة حيث قال مشرعون أمريكيون إن جهاز الأمن الأمريكي سيكشف عن تقدير لعدد المواطنين الذين التقطت اتصالاتهم الإلكترونية أثناء برامج المراقبة للإنترنت وذلك تحسبا من ان تكون هناك اتصالات مشبوهة بها خاصة ان التنظيمات الارهابية تستقطب مقاتليها عبر الاتصالات الالكترونية.

ايضا قام مكتب التحقيقات الامريكي (إف.بي.آي) بطلب بيانات اتصالات سرية وبعض أنواع سجلات الإنترنت من شركة تويتر واستشهدوا بأمرين للمراقبة بدون الحصول على تصريح رسمي نشرتهما شركة التواصل الاجتماعي وتصدر عادة مع أمر بالسرية بما يعني أن الهدف لا يدرك عادة أنه يجري الوصول إلى سجلاته وأنها لا تتطلب أمرا قضائيا. هذا ماأثار غضب خبراء قانونيون وقالوا ان مكتب التحقيقات الامريكي قد تجاوز فيما يبدو نطاق التوجيهات القانونية الحالية[1].

وكشفت وكالة المخابرات المركزية الأمريكية عن قواعد معدة لجمع المعلومات عن المواطنين الأمريكيين وتحليلها وتخزينها فيما يمثل تحديثا للقواعد يتماشى مع عصر المعلومات ونشرها بالكامل للمرة الأولى. و وكالة المخابرات المركزية الأمريكية مكبلة إلى حد كبير في شأن جمع المعلومات داخل الولايات المتحدة وعن المواطنين الأمريكيين.

بالرغم من الاجراءات المتشددة التي تتخذها الاستخبارات الامريكية مع الشعب الامريكي وطرق التجسس المتطورة المستخدمة معهم حتى في وسائل التواصل التي تعتبر من اكثر الامور خصوصية لكن معلومات وكالة الامن القومي الامريكي سربت من قبل موظف امريكي يبلغ من العمر 52 عام عمل لحساب وكالة الأمن القومي ووكالات حكومية أميركية أخرى، حيث قام الرجل المقيم في ولاية ماريلاند المحاذية للعاصمة الفدرالية واشنطن بنسخ وسلب معلومات سرية قدر حجمها بما لا يقل عن 50 ألف غيغابايت من البيانات والوثائق، بما في ذلك أدوات حساسة لقرصنة حواسيب حكومات أجنبية، سلبها من الوكالة على مدى عشرين عاما.

من جانب اخر في الوقت الذي اتهمت اجهزة الاستخبارات الاميركية موسكو بالوقوف وراء قرصنة معلوماتية ساعدت في فوز دونالد ترامب في الانتخابات الرئاسية، اعتقلت السلطات الروسية مسؤولين اثنين في

---

[1] ليو كليون، ويكيليكس: **المخابرات الأمريكية تستخدم أجهزة التلفاز الذكية للتجسس**، مقال منشور على الانترنت (مصدر) تاريخ الدخول: 2018/04/07
www.bbc.com/arabic/science-and-tech-39201722

الاستخبارات الروسية مختصين بالجرائم الالكترونية وخبيرا في القرصنة المعلوماتية ووجهت اليهم تهمة الخيانة من خلال العمل لصالح الولايات المتحدة.

على صعيد اخر قال خبراء قانونيون إن مكتب التحقيقات الاتحادي الأمريكي (إف.بي.آي) تجاوز فيما يبدو نطاق التوجيهات القانونية الحالية في طلبه بعض أنواع سجلات الإنترنت من شركة تويتر خلال العام الماضي واستشهدوا بأمرين للمراقبة بدون الحصول على تصريح رسمي نشرتهما شركة التواصل الاجتماعي.

وقالت تويتر إن هذا الكشف من جانبها بمثابة المرة الأولى التي يسمح لها بالكشف علانية عن الأوامر السرية التي سلمت لها مع أوامر بالتكتم عندما صدرت في 2015 و 2016. ويأتي هذا الإعلان عقب كشف مماثل في الشهور الأخيرة من قبل شركات إنترنت كبرى أخرى ومن بينها جوجل وياهو[1].

ويطلب كل من هذين الأمرين الجديدين ويعرفان باسم خطابات الأمن الوطني تحديدا نوعا من البيانات تعرف بسجلات حركة الاتصالات الإلكترونية والتي يمكن أن تتضمن بيانات عناوين رسائل البريد الإلكتروني وتاريخ التصفح من بين معلومات أخرى. وبذلك تعزز هذه الأوامر الاعتقاد بين المدافعين عن الخصوصية بأن مكتب التحقيقات الاتحادي استخدم في المعتاد خطابات الأمن الوطني لطلب سجلات الإنترنت خارج الإطار المحدد في المذكرة القانونية لوزارة العدل لعام 2008والتي خلصت إلى أن مثل هذه الأوامر يجب أن تقتصر على سجلات الفواتير الهاتفية. بحسب رويترز.

وفي تدوينة تكشف عن خطابي الأمن الوطني قالت شركة تويتر إنها لم تسلم كل المعلومات التي طلبها مكتب التحقيقات الاتحادي. وهذه الأوامر متاحة كأداة لسلطات إنفاذ القانون منذ السبعينات ولكن معدلها ونطاقها زاد بشكل كبير منذ صدور قانون باتريوت بعد وقت قصير من هجمات 11 سبتمبر عام 2001. وتصدر عشرات الآلاف من هذه الأوامر سنويا.

من جهتها قالت كارولين كراس المستشارة العامة لوكالة المخابرات المركزية الأمريكية في إفادة بمقرها في لانجلي بولاية فرجينيا إن المبادئ التوجيهية تم صياغتها "بأسلوب يحمي الخصوصية والحقوق المدنية للشعب الأمريكي." ونشرت القواعد الجديدة في ظل استمرار القلق العام بشأن سلطات المراقبة الحكومية وهي القضية التي سلطت عليها الأضواء بعد ما كشفه إدوارد سنودن المتعاقد السابق بوكالة الأمن القومي الأمريكية في عام 2013 عن جمع الوكالة سرا لبيانات ملايين من المواطنين الأمريكيين العاديين.

[1] ليو كليون، ويكيليكس: **المخابرات الأمريكية تستخدم أجهزة التلفاز الذكية للتجسس**, مقال منشور على الانترنت (مصدر) تاريخ الدخول: 2018/04/07
www.bbc.com/arabic/science-and-tech-39201722

ونشرت المبادئ التوجيهية قبل يومين من تنصيب الرئيس الأمريكي المنتخب دونالد ترامب وربما تغيرها الإدارة الجديدة. وكان ترامب عبر عن رغبته في توسيع صلاحيات المراقبة الحكومية لتشمل مراقبة مساجد "محددة" داخل الولايات المتحدة. وتتضمن الإجراءات الجديدة ما ينبغي على المخابرات المركزية القيام به عندما تصادر سرا قرصا ثابتا للكمبيوتر عليه ملايين الصفحات من النصوص وساعات من لقطات الفيديو وآلاف من الصور التي تتضمن معلومات عن أجانب وعن مواطنين أمريكيين. بحسب رويترز.

وبسبب الوقت الطويل والعدد الكبير من المحللين الذي يتطلبه تقييم مثل تلك المجلدات الضخمة من البيانات تنظم القواعد الجديد سبل معالجة المواد التي لا يمكن على الفور تقييم قيمتها المخابراتية. كما تحدد القواعد كيفية البحث في تلك البيانات وتضع متطلبات صارمة للتعامل مع الاتصالات الإلكترونية التي لم تخضع للتقييم بعد على أن يتم التخلص منها بصورة نهائية خلال مدة لا تتجاوز خمسة أعوام من يوم البدء في فحصها.

في السياق ذاته قال مشرعون أمريكيون في رسالة اطلعت عليها رويترز إن جهاز الأمن الأمريكي سيكشف قريبا عن تقدير لعدد المواطنين الذين التقطت اتصالاتهم الإلكترونية أثناء برامج المراقبة للإنترنت التي تستهدف أجانب .وسيجيء الإعلان في وقت من المتوقع أن يبدأ فيه الكونجرس نقاشا في الأشهر القادمة حول ما إذا كان ينبغي أن يجيز مرة أخرى ما يطلق عليه سلطة المراقبة أو القسم 702 وهو بند أضيف إلى قانون المراقبة الاستخباراتية للأجانب عام 2008.

وتقول الحكومة منذ فترة إن إحصاء عدد الأمريكيين الذين سرى عليهم القسم 702ربما يكون مستحيلا من الناحية الفنية. وكان مسؤولون بالمخابرات قد قالوا إنه "تصادف" جمع بيانات إلكترونية خاصة بأمريكيين وفقا للقسم 702 لعدة أسباب فنية وعملية. وانتقد البعض هذا الأمر بقوة ووصفوه بأنه مراقبة خفية للأمريكيين دون تفويض. بحسب رويترز.

وسينتهي العمل بالقسم 702 في 31 ديسمبر 2017 ما لم يتخذ الكونجرس إجراء. وهو يسمح باستخدام برنامجين للمراقبة على الإنترنت تم الكشف عنهما في سلسلة تسريبات لإدوارد سنودن المتعاقد السابق مع وكالة الأمن القومي الأمريكي منذ أكثر من ثلاث سنوات.

من جانب اخر أقر مجلس الشيوخ الأمريكي تعيين مرشح الرئيس الأمريكي دونالد ترامب النائب مايك بومبيو لمنصب مدير وكالة المخابرات المركزية الأمريكية وقد صوت 66 عضوا لصالح بومبيو بينما صوت 32 عضوا ضده. وجاءت كل المعارضة من الديمقراطيين باستثناء راند بول وهو جمهوري بارز يؤيد فرض قيود صارمة على المراقبة. وبعد ذلك بقليل أدى بومبيو اليمين.

وشعر بعض أعضاء مجلس الشيوخ أن بومبيو (53 عاما) لم يتعهد بقوة كافية بأن يسمح فقط باستخدام أساليب التحقيق المتضمنة في الدليل الإرشادي الميداني للجيش كما يقضي القانون بدلا من العودة إلى الإيهام

بالغرق و"أساليب الاستجواب المعززة" التي استخدمتها وكالة المخابرات المركزية الأمريكية في السنوات التالية لهجمات 11 سبتمبر.

وقال بومبيو ردا على أسئلة مكتوبة من لجنة المخابرات بمجلس الشيوخ إنه مستعد لتغيير السياسة في ظل ظروف معينة. وكتب يقول "سأتشاور مع خبراء فيما إذا كان التطبيق الموحد للدليل الميداني للجيش عائقا أمام الحصول على معلومات حيوية لحماية البلاد." وتحدث السناتور رون وايدن لأكثر من ساعة في مجلس الشيوخ معارضا ترشيح بومبيو قائلا إنه قدم إجابات متضاربة فيما يتعلق بالمراقبة وأساليب الاستجواب مما يجعل من المستحيل معرفة كيف سينفذ السياسة في وكالة المخابرات المركزية. بحسب رويترز.

ووصف معظم الجمهوريين بومبيو وهو عضو في لجنة المخابرات في مجلس النواب بأنه اختيار ممتاز. وقال السناتور جون مكين وهو من متصدري المعركة من أجل تشريع يحظر استخدام أساليب الاستجواب القاسية "ليس لدي ما يدعو للشك في وعد عضو الكونجرس بومبي.

ليس من المرجح أن تتراجع عمليات حرب المعلومات الدائرة بين روسيا والدول الغربية، فموسكو تصر على الحفاظ على نفوذها التقليدي وإرثها في الدول التي كانت ضمن المجال السوفيتي، وبالتالي فإن تقدم الغرب إلى هذه المناطق واستقطابه لهذه الدول سيدفع روسيا –بشكل أو بآخر– إلى التكريس لمدخل الحرب الهجينة Hybrid Warfare، والتي تمتزج فيها الأدوات التقليدية وغير التقليدية، في تعاطيها مع الغرب، وخاصة مع تراجع إمكانية اللجوء إلى الخيار العسكري التقليدي في التعامل مع الولايات المتحدة والدول الأوروبية . وتُعزز التحولات الراهنة في النظام الدولي هي الأخرى من تفعيل أدوات حرب المعلومات، فمع تعرض الولايات المتحدة لأزمات أثناء السنوات الماضية، والشكوك حول استمرارية قيادتها المنفردة للنظام الدولي، وبزوغ قوى منافسة مثل روسيا طامحة في المشاركة في قيادة هذا النظام، سيكون لحرب المعلومات جاذبيتها في إدارة العلاقات بين هذه القوى المتنافسة.

المبحث الثاني: الردود الأمريكية على القرصنة الروسية

منذ المراحل الأولى لتطور الإنترنت، اعتبرت مؤسسة الأمن القومى الروسى أن الإنترنت هو بمثابة سلاح يمكن من خلاله تغيير النظم السياسية وصعوبة مهمة الدولة فى فرض سيادتها على أراضيها. تضم منظمة Russia's information warfare capabilities مستخدمى الإنترنت ومنافذ إعلامية ومتصيدى وسائل التواصل الاجتماعى، وكل هؤلاء محاطين بدرجة عالية من السرية.

من الجدير بالذكر أن الحكومة الروسية تمتلك العديد من الجهات الفاعلة فى الحرب السيبرانية، وذلك من خلال توظيف مستأجرين ومجرمين سابقين لينفذوا هذه العمليات، مما يعطى لموسكو الحق فى نفى ذلك إذا تم اكتشافهم وقبض عليهم .

ومع ذلك يمكن للحكومات الغربية والقطاع الخاص أن يأخذوا خطوات للتحقق من عمليات النفوذ الروسى.ويجب عليهم أن يتهموا بشكل قاطع الأنشطة الروسية بمجرد أن يتم تحديدها. كما ينبغى على وكالات مكافحة التجسس أن تحدد الوسائل الكمية لقياس فعالية المناهج الروسية فضلا عن ضرورة أن تقوم شركات التواصل الاجتماعى بمزيد من الرقابة على مواقعها للمحتويات الذى ترعاها الدولة المعادية. كما يجب على المؤسسات الإخبارية أن تروج للمحتويات التي يتم التحقق منها وإثبات صحتها على مواقعها.

يكمن هدف السياسة الخارجية الروسية فى إضعاف خصومها، خاصة الدول المتاخمة لحدودها وحلف الناتو والولايات المتحدة الأمريكية، وذلك بأى وسيلة متاحة .وتستهدف حربها المعلوماتية التماسك الاجتماعى والنظم السياسية للدول المعادية .

خلال القرن العشرين استغل الاتحاد السوفيتي حرية التعبير فى الغرب وقام بزرع ونشر الأخبار الزائفة، وفى العقد الأخير فإن صعود وسائل التواصل الاجتماعى جعلت هذه المهمة أبسط من ذى قبل بكثير؛ فمنذ عام 2017، استغلت موسكو شبكات الإعلانات المتطورة والتى تستخدمها الشركات المشروعة والحملات السياسية من أجل تضليل الجمهور المستهدف .

حُرم فلاديمير بوتين من القدرات الضخمة التي كان يتوفّر عليها المجمّع الصناعي العسكري السوفيتي، لذلك بحث طويلا عن مجال أقلّ كلفة، يسمح للروس بتجاوز الأميركيين، ومن هنا خطرت على باله فكرة الردّ اللاّتناظري أو الرد غير التقليدي على الولايات المتحدة.

ويندرج هذا الرد منذ 2014 ضمن عقيدة عسكرية روسية، صمّمها قائد الأركان الروسي فاليري غيراسيموف، وتقوم هذه العقيدة على ردود عسكرية لا تناظرية، أي على حرب هجينة، تعتمد على فعالية الحرب الالكترونية.

قامت روسيا باختبار هذه العقيدة الجديدة على جيرانها، قبل ادراجها ضمن خطتها العسكرية، حيث طبقتها في استونيا في عام 2007 ثم جورجيا في 2008، فأوكرانيا في 2014. وقد سقطت هذه الدول

الثلاث ضحية هجمات الكترونية كبيرة من طرف روسيا، وقد خبر العالم القدرات الروسية الجديدة خلال الحملة الرئاسية الأميركية، حيث اتفق خبراء الأمن الالكتروني الغربيون بعد تعقبهم للهجمة الالكترونية التي استهدفت اللجنة الوطنية لحزب الديمقراطيين على تورط مجموعة قراصنة يطلق عليها اسم «فانسي بير .«وهذه المجموعة غير الرسمية، التي أسست في عام 2007، هي المسؤولة أيضا عن نشر معلومات سرية عن رياضيين أميركيين ردا على فضيحة تناول رياضيين روس للمنشطات ومجموعة فانسي بير متورطة أيضا في هجوم استهدف الخوادم التابعة لمنظمة الامن والتعاون في اوروبا.

عملت روسيا على تحقيق هذا الهدف خلال الحملة الانتخابية الأمريكية فى 2016، عندما مزجت الوكالات الروسية بين العوامل التقنية والنفسية للتأثير على الناخبين الأمريكين ليصوتوا لصالح مرشح الحزب الجمهورى «دونالد ترامب». حيث قام القراصنة الروس بنشر وثائق تدين مرشحة الحزب الديمقراطى «هيلارى كيلنتون «من أجل إحراج حملتها الانتخابية فضلا عن أن وسائل التواصل الاجتماعى لعبت دورا فى هذا النطاق من خلال متصيدى وسائل التواصل الاجتماعى مما أدى إلى تعزيز فرص نجاح «ترامب.«

كشف وكالة المخابرات المركزية "سي آي إيه" أن اثنين من القراصنة الروس المدعومين من الحكومة الروسية، قاما باختراق خوادم اللجنة الوطنية الديمقراطية خلال عاميّ 2015 و2016، بحسب تقرير نشرته صحيفة نيويورك تايمز.

وأشارت "سي آي إيه"، في تقريرها الصادر في ديسمبر من العام الماضي، إلى أن القراصنة الروس قاموا بإنشاء منافذ على شبكة الإنترنت جعلت وثائق اللجنة الديمقراطية متاحة للجميع.

وأثار تسريب الوثائق موجة غضب واسعة عصفت الديمقراطيين، كما دفع رئيسة الحزب الديمقراطي الأمريكي، ديبي ويسرمان شولتز، إلى تقديم استقالتها، وهو الأمر الذي أجّج بدوره الصراع بين داعمي السيناتور بيرني ساندرز وهيلاري كلينتون.

وتسبّب اختراق البريد الإلكتروني لرئيسة حملة مرشحة الرئاسة عن الحزب الديمقراطي هيلاري كلينتون، في كشف النقاب عن الديناميات الداخلية لحملتها خلال فترة السباق الرئاسي أمام الجمهوري دونالد ترامب،

واعتبرت إدارة أوباما أن الاختراق الروسي للجنة الديمقراطية يمثل تدخلًا دوليًا واضحًا في العملية الانتخابية، وَفق ما أوردته صحيفة "ذا هيل" الأمريكية.

في سبتمبر، وجّه الرئيس المنتهية ولايته باراك أوباما تحذيرًا لنظيره الروسي فلاديمير بوتين من محاولة التلاعب في الانتخابات الأمريكية، أعقبه فرض عقوبات من جانب إدارة أوباما على وكالتيّ استخبارات، وأربعة مسؤولين، وثلاث شركات في روسيا، فضلًا على طرد 35 دبلوماسيًا روسيًا وعائلاتهم من البلاد، في الوقت الذي يزعم فيه بعض المسؤولين صلتهم بهجمات القرصنة الأخيرة.

كما أغلقت وزارة الخارجية الأمريكية اثنين من المرافق المستخدمة من جانب الاستخبارات الروسية في مدينة نيويورك بولاية ماريلاند، بحسب "نيويورك تايم

وفرضت الإدارة الأمريكية عقوبات اقتصادية على جهازي الامن الفدرالي «اف اس بي» واستخبارات الجيش «جي آر يو» الروسيين وعلى اربعة مسؤولين في «جي آر يو» من بينهم رئيسه ايغور كوروبوف

أوضح اوباما ان العقوبات لن تتوقف عند هذا الحد، محذرا من إن الولايات المتحدة ستتخذ اجراءات اخرى من بينها عمليات سرية لن يتم اطلاع الراي العام عليها. وتابعت واشنطن ان الاجراءات المعلنة رد ايضا على «المستوى غير المقبول من المضايقات» التي يتعرض لها الدبلوماسيون الأمريكيون منذ عام في موسكو من قبل الشرطة او اجهزة الاستخبارات الروسية على ما تؤكد واشنطن.

كما وجه اوباما نداء لتشكيل نوع من الوحدة الدولية لاعادة موسكو الى الطريق الصحيح ولئلا تتخذ اي اجراءات من شانها زعزعة الاستقرار في دول اجنبية

فقد أصدرت وزارة الأمن الداخلي الأمريكية بيانًا هامًا تمثل في أول اتهام مباشر توجهه إدارة أوباما ضد روسيا بأنها تسعى للتدخل في الانتخابات الأمريكية، وقد ورد في البيان ما يلي: "الأجهزة الاستخبارية الأمريكية واثقة من أن الحكومة الروسية قد أمرت مؤخرًا بكشف رسائل إلكترونية لمواطنين ومؤسسات أمريكية بما في ذلك تلك القادمة من منظمات سياسية أمريكية، وذلك بغاية التأثير على نتائج الانتخابات" فبعد أن تعرضت اللجنة القومية الديمقراطية وآلات التصويت للقرصنة، وبعد أشهر من الحديث في الصحافة وفي الكابيتول هيل، فإن إدارة أوباما توجه إصبع الاتهام للكرملين بكونه يحاول التدخل في الانتخابات الأمريكية.

وقد كان ذلك على إثر تسريب جديد لعدد من الوثائق من ويكيليكس تحتوي على رسائل إلكترونية لمدير حملة هيلاري كلينتون جون بوديستا، كما تم تسريب أخبار تفيد بأن السفير الروسي لدى الأمم المتحدة كان قد تقدم بشكوى رسمية لدى المنظمة بعد أن انتقد مسؤول آخر المرشح الجمهوري ترامب، ويأتي كل هذا على خلفية ثناء ترامب المستمر والمفرط على فلاديمير بوتين، وكذلك على خلفية انتشار معلومات تفيد بوجود علاقات مشبوهة تربط حملة ترامب بروسيا

ومن جانبها، أرجعت وزيرة الخارجية الأمريكية السابقة هيلاري كلينتون سبب خسارتها الانتخابات الرئاسية إلى القرصنة الروسية .وقالت في حفل لمانحيها إن بوتين لديه "حنق شخصي" تجاهها لوصفها الانتخابات البرلمانية الروسية قبل خمس سنوات بالمزيفة.

ونسبت لها صحيفة نيويورك تايمز القول:"ألقى بوتين اللوم علي عندما استشرى الغضب بين شعبه، وهذا هو الخط المباشر بين ما قاله في ذلك الوقت، وما فعله في تلك الانتخابات ".

وأضافت قائلة: "إن ما حدث ليس هجوما على شخصي وعلى حملتي فحسب بل هو هجوم على بلدنا، فهذا الأمر يتجاوز السياسة ويتعلق بديموقراطيتنا وأمن أمتنا.

وفي مقال له نشر في صحيفة لوفيغارو، قال الاستاذ في جامعة السوربون ومؤلف كتاب «الاميركيون» اندري كاسبي، إن العالم لم يشهد اليوم حربا باردة جديدة بين الولايات المتحدة وروسيا تشبه ما حصل قبل 40 او 50 عاما، وأما شعلتها الاولى فتتمثل في طرد الولايات المتحدة لـ35 دبلوماسيا روسيا بتهمة قرصنة مواقع الكترونية والتأثير على اتجاهات الناخبين، وأضاف الأكاديمي ذاته "بين واشنطن وموسكو يتزايد التحدي والعداء أيضا، ففي بداية ولايته، كان أوباما يعتقد بأنه سيستطيع التفاهم مع بوتين، ولكنه اكتشف في ما بعد بأنه مخطئ، حيث حوّل ضمُّ شبه جزيرة القرم والتدخلُ في أوكرانيا والتهديدات التي تعاني منها دول البلطيق، حوّل روسيا إلى قوة خطرة في عيون الاميركيين"

ويقول أندري كاسبيان إن طرد الولايات المتحدة لجواسيس روس يشبه إلى حد بعيد عملية اتصال لأن الدافع الحقيقي لأوباما هو شيء آخر تماما.

لقد فاجأ فوز ترامب المراقبين ويمكن أن يكون قد فاجأ ترامب نفسه، لكن هذا الفوز يوضح فشل أوباما، الذي قاد برفقة زوجته حملة لمصلحة هيلاري كلينتون، ورغم ذلك قرر الاميركيون غير ذلك، والنتيجة اتخاذ أوباما لسلسلة قرارات تهدف إلى إضعاف الرئيس المقبل، وأبرزها الامتناع عن التصويت لمصلحة قرار يدين الاستيطان الاسرائيلي بينما تعهّد ترامب بنقل السفارة الأميركية إلى القدس وعيّن المحامي ديفيد فريدمان المؤيد لليمين الإسرائيلي سفيرا لواشنطن في إسرائيل ومنع التنقيب عن النفط في الاطلنطي ومنطقة القطب الشمالي، على الرغم من دفاع ترامب عن الوقود الأحفوري وأمر بإحياء ذكرى بيرل هاربور بعد مرور 75 عاماً على الغارة الجوية المباغتة التي نفذتها البحرية الإمبراطورية اليابانية على الأسطول الأميركي القابع في المحيط الهادئ في قاعدته البحرية في ميناء بيرل هاربر بجزر هاواي، ما أعطى الانطباع بأن العلاقات التجارية والسياسية بين طوكيو والبيت الابيض لا يمكن التشكيك فيها، خصوصاً مع تعاظم التهديد الاقتصادي والعسكري الصيني

عبر الرئيس الأمريكي المنتخب دونالد ترامب عن شكوكه فيما توصلت إليه وكالات المخابرات الأمريكية بأن روسيا تقف وراء عمليات القرصنة التي استهدفت الحزب الديمقراطي خلال الحملة الانتخابية الرئاسية العام 2016 .يأتي ذلك قبل يوم واحد من استقبال ترامب لمديري وكالات المخابرات لإطلاعه على عمليات الاختراق الإلكتروني التي استهدفت الحزب الديمقراطي.

ويلوح صراع بين ترامب والديمقراطيين وأعضاء حزبه الجمهوري في الكونغرس الذين يشعر كثير منهم بالقلق من روسيا ولا يثقون في مديح ترامب للرئيس الروسي فلاديمير بوتين وجهوده لرأب الصدع بين الولايات المتحدة وروسيا.

وتقول وكالات المخابرات الأمريكية إن روسيا كانت وراء عمليات اختراق لمنظمات تابعة للحزب الديمقراطي وعمليات سرية قبل الانتخابات الرئاسية وهو استنتاج أيدته عدة شركات خاصة تعمل في مجال أمن المعلومات. وتنفي موسكو تلك المزاعم.

وقال مسؤولون بالمخابرات الأمريكية إن عمليات الاختراق الروسية كانت تهدف لمساعدة ترامب على إلحاق الهزيمة بمنافسته الديمقراطية هيلاري كلينتون في الانتخابات الرئاسية التي أجريت في الثامن من نوفمبر/ تشرين الثاني .ويعتقد عدد من الجمهوريين بحدوث تسلل إلكتروني خلال الانتخابات لكنهم لم يربطوا ذلك بمسعى لمساعدة ترامب على الفوز.

وكانت وثائق سرقت من اللجنة الوطنية الديمقراطية ومن جون بوديستا مدير حملة كلينتون قد سربت إلى وسائل الإعلام قبل الانتخابات ما سبب حرجا لحملة كلينتون.

وقدم خمسة ديمقراطيين بمجلس الشيوخ تشريعا يدعو لإنشاء لجنة مستقلة غير حزبية للتحقيق بشأن التدخل الروسي في الانتخابات.

ورشح ترامب أشخاصا تعتبر مواقفهم ودية تجاه موسكو لمناصب قيادية في إدارته من بينهم ريكس تيلرسون المرشح لوزارة الخارجية الذي قلده بوتين وسام الصداقة العام 2013 أثناء توليه الرئاسة التنفيذية لشركة إكسون موبيل

وتمسك ترامب بأنه فاز في الانتخابات بنزاهة وانتقد التلميحات إلى أن موسكو أثرت على النتيجة. وفي وقت ما أثناء الحملة الرئاسية المحتدمة شجع ترامب روسيا علنا على التسلل إلى البريد الإلكتروني لكلينتون.

وتحدث ترامب بنبرة إعجاب خلال حملته الانتخابية عن بوتين واختار منذ فوزه بالانتخابات مساعدين كبارا في حكومته على صلة بروسيا .

".انتقدت مستشارة الرئيس الاميركي المنتخب دونالد ترامب، كيليان كونواي العقوبات الاميركية الاخيرة على روسيا معتبرة انها ربما تهدف الى "التضييق على" خلف باراك اوباما في البيت الابيض.

وقالت كونواي لشبكة سي ان ان "بحسب اعتقادي لم يطرد هذا البلد هذا القدر من العناصر حتى في اوج الحرب الباردة" ووصفت العقوبات بانها "غير مسبوقة."

ولم تطرد الولايات المتحدة هذا القدر من الدبلوماسيين الروس منذ 2001، مع ترحيل 50 مسؤولا روسيا اتهموا بالاتصال بالعنصر في مكتب التحقيقات الفدرالي روبرت هانسين الذي عمل لصالح الروس لمدة 15 عاما.

واشارت كونواي الى اعتقاد كثيرين ان الغرض من العقوبات "التضييق" على ترامب وتقليص هامش المناورة الذي يملكه ازاء روسيا مع حلول موعد تنصيبه رسميا في 20 كانون الثاني/يناير 2016.

وقالت "سيكون مؤسفا ان اتضح ان السياسة هي الدافع الرئيسي" للعقوبات مضيفة "هذه ليست طريقة اجراء عمليات تبادل سلمية في هذه الديموقراطية

وتجاهل ترامب اتهامات وكالة المخابرات المركزية الأمريكية ووكالات مخابرات أخرى بأن روسيا هي المسؤولة عن الهجمات الإلكترونية. وقال إنه سيجتمع مع مسؤولي المخابرات قريبا.

وقال ترامب في بيان **"حان الوقت كي تتحرك بلادنا إلى أشياء أكبر وأفضل"**.

وأضاف من دون ذكر روسيا "ومع ذلك ومن أجل صالح بلدنا وشعبها العظيم فسوف أجتمع مع قادة المخابرات من أجل الإطلاع على حقائق هذا الموقف

أما الآن، فنحن نشهد حملة أخرى تقودها روسيا في الولايات المتحدة، لا شيء حقيقي، ولا شيء قابل للإثبات، مع استثناء لكل ما هو غير محتمل وغير قابل للإثبات (هذا يذكرنا بنشر صحيفة موالية للكرملين مقالاً يتحدث عن أن الرئيس الأوكراني بيترو بوروشينكو عقد اتفاقًا، مدعين أن لروسيا وثيقة الاتفاق وأن توقيعات الجانبين كانت "حقيقية")، وبالنسبة لترامب، فإن حياته خارج حدود الحقيقة وإتقانه لأسلوب الدعايات شبيه إلى حد كبير بسياسات بوتين.

وإن أدركت روسيا في وقت سابق بأن النظام السياسي للولايات المتحدة شبيه إلى حد ما بالنظام السياسي الروسي، لكانت بدأت مهمتها منذ وقت طويل، ووفقًا لمايكل إيزيكوف، فإن بوتين له مستشار يدعى إيغون ديفايكيف، وهو ضابط مخابرات سابق يشرف الآن على "المعلومات الاستخباراتية التي جمعتها وكالات الاستخبارات الروسية فيما يتعلق بالانتخابات الأمريكية"، وكان أحد عملاء الاستخبارات الأمريكية قد قال متحدثا لـ "آن بي سي" إن برنامج المخابرات المتعلق بالولايات المتحدة تم إنشاؤه منذ سنتين، لكنه بدأ في العمل منذ سنة واحدة، أي أن هذا البرنامج جديد.

– المبحث الثالث: السيناريوهات المستقبلية للصراع السيبراني الأمريكي – الروسي .(تصاعد الصراع – إنخفاض الصراع)

أن معظم الاتفاقيات الدولية ذات الصلة بتنظيم استخدام وسائل و طرائق القتال ، أبرمت في زمن لم يكن معروفاً خلالها، استخدام الانترنت أو وسائل الاتصال الالكترونية كما هو الحال في الوقت الراهن ، ومن الطبيعي أن لا نجد حكماً قانونياً ينظم استخدام الهجمات السيبرانية بشكل صريح ومباشر. لا يعني أيضاً أن يترك الباب مفتوحاً أمام الهجمات السيبرانية دون تنظيم قانوني، وهو الأمر نفسه يذكرنا بعدد من الأسلحة التي تم تنظيمها لا وفقاً لقواعد ومبادئ قانونية مدونة، إنما وفقاً لقواعد دولية عرفية راسخة في التنظيم الإنساني الدوليوفي السياق نفسه، يمكن الاستناد إلى ما أصدرته محكمة العدل الدولية من فتوى بشأن شرعية التهديد أو استخدام الأسلحة النووية في عام 1996 ، في ضوء المبادئ الدولية، كمبدأ أن حق أطراف النزاع في اختيار وسائل و طرائق القتال ليس حقاً مطلقاً، ما يعني أن الفرصة سانحة أمام المجتمع الدولي لتنظيم هذا الموضوع بالاستناد إلى المبادئ نفسها، فضلاً عن الاسترشاد بالاتفاقيات الدولية والتشريعات الداخلية
التي نظمت موضوع مكافحة الجرائم السيبرانية.

وقد يتساءل البعض ، لم لا يتوصل المجتمع الدولي – في الوقت الراهن – إلى إبرام اتفاقية دولية تحظر استخدام الهجمات السيبرانية أو تقييد استخدامها في اقل تقدير؟

أن الإجابة عن هذه الإشكالية، تتطلب تفحص المصالح الدولية التي تقف حائلاً دون إبرام مثل هكذا اتفاقيات دولية، وبعبارة أخرى مصالح الدول التي تحتكر أو تهيمن على قطاع البرامج الالكترونية للأغراض العسكرية؟

أن التفوق الذي تتميز به بعض الدول كالولايات المتحدة وروسيا الاتحادية في حقل الأنظمة الالكترونية العسكرية والمهيمنة على الساحة الدولية، أدخل موضوع الهجمات السيبرانية ضمن دائرة الصراعالتقليدي الذي كان دائرا بينها في أثناء زمن الحرب الباردة، وبعبارة أخرى الرجوع إلى مفهوم الهيمنة من أجل النفوذ وتحقيق كل منهما مكاسب محددة سلفاً، قبل الخوض في مسألة تنظيمه بصيغة اتفاقية دولية متعددة الأطراف. وكالعادة فإن التحدي الأكبر الذي يواجه تنظيم الهجمات السيبرانية هو عدم وجود إرادة دولية على الصعيدين الدبلوماسي) المفاوضات (والقانوني) قرارات مجلس الأمن (، يقابله تسارع وتيرة استحداث وتطوير أنظمة الكترونية قادرة على التسلل والاختراق لأنظمة الكترونية تابعة لدولة أخرى ، ومن ثم إلحاق الضرر بها على نحو يمكن وصفه هجوماً وعدواناً مباغتاً للمنشآت الحيوية

أن الخطورة الكامنة في اللجوء إلى الهجمات السيبرانية، دفع بالجمعية العامة للأمم المتحدة إلى إيلاء اهتمام كبير بحث الدول قُدماً نحو بدء مفاوضات دولية و تنظيم استخدامها وفقا لأحكام القانون الدولي

الإنساني، من خلال سلسلة من القرارات صدرت عنها، وبقيت في طي الوثائق دون أن تجد لها صدى في

المحافل الدولية المعنية ببدء المفاوضات الدولية و السبب في تأخر إبرام معظم الاتفاقيات ذات الصلة بوسائل و طرائق القتال، يعود إلى عدم رغبة الدول المعروفة بصناعاتها العسكرية المتقدمة في الدخول إلى اتفاقيات دولية، قد تحظر عليها وسائل تساعد في حفظ أمنها تحت مسميات الضرورة العسكرية،هذه المعضلة دفعت بالأمم المتحدة و بعض الدول للإعلان صراحةً عن نيتها بدعم أي توجه دولي يفضي إلى حظر أو تقييد استعمال أنظمة الكترونية معدة للاستخدام العسكري أو الأمني،و وفقاً لما استقر عليه القانون الدولي العام المقنن، فضلاً عن العرف الدولي والسوابق القضائية وآراء كبار فقهاء القانون. و يعد الأمين العام للأمم المتحدة بان كي مون أول مسؤول أممي، دعا لإبرام اتفاقيةدولية متعددة الأطراف، تنظم مسألة الهجمات السيبرانية، فيما أيدت وزارة الخارجية الأمريكية هذا التوجه ، وصرحت أن النموذج الأفضل والواجب الاقتداء به في إبرام الاتفاقية الدولية، هو اتفاقية مجلس أوربا المتعلقة بالجريمة السيبرانية لعام 2001 فالولايات المتحدة الأمريكية تحبذ السير على النهج ذاته المتبع في اتفاقية مجلس أوربا المتعلقة بالجريمة السيبرانية لعام 2001، لإبرام اتفاقية دولية تنظم استخدام الهجمات السيبرانية على صعيد النزاعات المسلحة تناولت الاتفاقية موضوع التعاون الدولي الجرائم السيبرانية وذلك في القسم الثالث منها، إذ نصت المادة) 23 (بأنه ":يتعاون الأطراف مع بعضهم البعض، وفقاً لنصوص هذا الباب ومن خلال تطبيق الاتفاقيات الدولية ذات الصلة والخاصة بالتعاون الدولي في الشؤون الجنائية والترتيبات المتفق عليها بمقتضى التشريعات والمتبادلة بالمثل، والقوانين الوطنية لأقصى درجة ممكنة لأغراض إجراءات التحقيقات التي تتعلق بجرائم نظم وبيانات الكومبيوتر، أو من أجل تجميع أدلة الجريمة الجنائية في شكل الكتروني"، كما تناولت المادة) 24 (من الاتفاقية مسائل ضرورية لإتمام التحقيقات من ضمنها مسألة تسليم المجرمين لكن ترى روسيا الاتحادية وعلى النقيض من التأييد الأمريكي للاتفاقية، أن اتفاقية مجلس أوربا لا يمكن الاعتماد عليها في مسألة تنظيم الهجمات السيبرانية لوحدها ، بل لا بد من إبرام اتفاقية دولية معنية بالهجمات السيبرانية، تأخذ في الحسبان القواعد الدولية المنظمة لسير النزاعات المسلحة، وعلى أن تصنف الاتفاقية ضمن مجموعة الاتفاقيات الدولية المعنية بالحد من) Internationalالتسلح وعنوانها المقترح هو الاتفاقية الدولية المعنية بالحد من الأسلحة السيبرانية

Cyber Arms Control Treaty192) . ومما تقدم من مواقف يبدو جلياً توجهات أكبر دولتين مهتمتين بالمجال العسكري السيبراني، فالولايات المتحدة تدعو إلى ما يمكن الاصطلاح عليه بنزع الأسلحة السيبرانية ،فيما تتجه النوايا الروسية إلى ابعد من ذلك وهو الحد منها. أن المقترح الروسي هذا يعود للعام 1998 ، عندما دعت الأخيرة الأمم المتحدة لآجل كبح الهجمات السيبرانية وهو ما دفع بالجمعية العامة للأمم المتحدة عام 2000 لإصدار قرار يدعو إلى دراسة التهديدات التي تصاحب استخدام المنظومات الالكترونية لإغراض عسكرية، وإمكانية السير باتجاه تبني معايير دولية للحد من مخاطرها على المستوى الدولي.

وكحال أية مبادرات دولية معنية بالحد من التسلح أو نزعه، تناوبت روسيا الاتحادية والولايات المتحدة الأمريكية الأدوار، عن طريق طرح عدد من المقترحات لأجل إبرام اتفاقية دولية متعددة الأطراف يضمن مصالح كل واحدة منهما، وهو ما يمكن بيانه لدى تحليل موقفهما من مشروع الاتفاقية وكالآتي

1- موقف روسيا الاتحادية:

و يركز على تبني اتفاقية دولية تضع في الحسبان مبدأ الامتناع في :

أ -تطوير أو استحداث أو استخدام وسائل التأثير أو الإضرار في الأنظمة والمصادر المعلوماتية للدول الأخرى.

ب -الاستخدام المتعمد للمعلومات بهدف التأثير أو الإضرار في المنشآت الحيوية للدول الأخرى.

ت -الدخول غير المصرح به في أنظمة المعلومات و الاتصالات ومصادرها، فضلاً عن استخدامها.

ث -مساعدة أو تشجيع المجموعات الإرهابية أو الأفراد الخارجين عن القانون لتهديد الدول عن طريق استخدام أنظمتها الالكترونية و وسائل الاتصال الأخرى

ج -حظر استخدام كلمات المرور الخبيثة في أثناء سير العمليات القتالية.

ح -حظر مهاجمة الأنظمة غير القتالية أو العمل على الخداع في عملها

2 .موقف الولايات المتحدة الأمريكية:

لو راجعنا موقف الولايات المتحدة من المقترح الروسي آنف الذكر، لاتضح تأييدها له في بداية الأمر، ولكن سرعان ما تبدل هذا التأييد ، لتمارس الولايات المتحدة مناورة اعتادت على إتباعها فيما يخص موضوعا نزع السلاح و الحد منه مؤخراً عن رغبة الولايات المتحدة في السعي لإبرام (Barack Obama) لقد أعلنت إدارة باراك اوباما اتفاقية دولية لا تحظر استخدام المنظومات الالكترونية في نطاق العمليات الأمنية أو العسكرية، بل بتقييد مع قبول الولايات المتحدة بدء محادثات ثنائية مع روسيا الاتحادية بشأن (Restriction) استخدامها تحديد المبادئ العامة للاتفاقية في إطار لجنة الأمم المتحدة لنزع السلاح والأمن الدولي أن الرغبة الثنائية في مسألة تنظيم الهجمات السيبرانية على هيئة اتفاقية دولية، قد حدث بالفعل عام 2010 من خلال محادثات جمعت الجانبين الأمريكي والروسي، وصفت بأنها الأولى من نوعها على صعيد الموضوع وهو تنظيم استخدام الهجمات السيبرانية أن التوجه الأمريكي يمكن تحديده من خلال الرأي الذي أبداه مدير وكالة الأمن القومي كيث الكسندر (Keith Alexander) عام 2010 ،بالقول" :نحن ماضون في تبني قواعد بشأن الحرب السيبرانية ونحن نعتقد بأن روسيا قد بدأت بالفعل تبني قواعد في المحادثات الدولية وفي ضوء ما تقدم من مواقف دولية وبالخصوص الأمريكية، يتضح أن لا اتفاقية مجلس أوربا المتعلقة بالجريمة السيبرانية لعام 2001 ، ولا المقترح الروسي القاضي بإبرام اتفاقية دولية تحظر الهجمات السيبرانية يسيران في اتجاه واحد، وإن مشوار المحادثات الثنائية

سيستغرق وقتاً طويلاً كما هو حال باقي المحادثات التي جرت على قضايا الحد من الأسلحة أو نزعها، و تبقى الإرادة الدولية هي المهيمنة على الأوضاع القانونية الدولية ، والسبب الرئيس في بطئ تطور القانون الدولي العام والإنساني بالخصوص.

أن إبرام اتفاقية دولية تنظم الهجمات السيبرانية، سيشهد عقبات ستضعها الدول العظمى وبالخصوص الولايات المتحدة وروسيا الاتحادية والصين، كما هو حال معظم المواضيع الدولية ذات الصلة بالسلم والأمن الدوليين والتي شهدت التعطيل لفترات طويلة." أن إبرام اتفاقية دولية تنظم الهجمات السيبرانية، سيشهد عقبات ستضعها الدول العظمى وبالخصوص

الولايات المتحدة وروسيا الاتحادية والصين، كما هو حال معظم المواضيع الدولية ذات الصلة بالسلم والأمن الدوليين والتي شهدت التعطيل لفترات طويلة وفي هذا الشأن يختصر الفقيه الألماني ماركو جيركه بطرحه تصوراً عن مستقبل الاتفاقية وبالذات فيما لو سارت على النهج نفسه المتبع في اتفاقية الجريمة السيبرانية لعام 2001 بالقول ": أن عقداً من الزمن مضى على إبرام اتفاقية الجريمة السيبرانية في أوربا، دون أن تلقى اتفاقية مماثلة خارج حدودها ، ما يعني أنها لم تكن ذات دور مؤثر في مكافحة الجريمة السيبرانية على النطاق العالمي.

بعد بيان مفهوم الهجمات السيبرانية من التنظيم الدولي المعاصر يتضح أنه ليس من المستغرب أن يتربع موضوع الهجمات السيبرانية، الصدارة في الدراسات القانونية المتخصصة بالقياس إلى القضايا الدولية ما يشكل إحدى أهم التحديات الراهنة التي يواجهها المختصون في القانون الدولي العام، وبالخصوص في تحديد طبيعتها أو عناصرها، فضلاً عن نطاق هذه الهجمات في ضوء القانون الدولي الإنساني وما يترتب عليها من تبعات المسؤولية الدولية وفيما لو تم الاتفاق على انطلاق المفاوضات متعددة الأطراف رسمياً بشأن الهجمات السيبرانية، فإن المسائل الأكثر إلحاحاً بالتنظيم ستدور في أحكام نطاق الاتفاقية وبعبارة أخرى خيار الحظر أم التقييد في الاستخدام،فضلا عن الأحكام ذات الصلة بامتثال الدول الأطراف للاتفاقية، وخصوصاً في حظر دعم المجموعات من غير الدول) المجموعات الإرهابية أو المجموعات المسلحة غير النظامية (ما يعني أن نتوقع عقداً من الزمن أو أكثر من المفاوضات لأجل إبرامها على المستوى الدولي متعدد الأطراف.

أن إبرام الاتفاقية على النحو الذي قصدناه آنفاً، سيعني تحريك المسؤولية الجنائية الفردية عن دعم أو تدريب أو تمويل أي مجموعات إرهابية يمكن أن تستخدم الوسائل الالكترونية للأغراض غير العسكرية تجاه دول أخرى.

الخـــــاتمـة

الخاتمة

لم تقتصر تأثيرات اختراق الثورة التكنولوجية مجالات الحياة المختلفة على التفاعلات المجتمعية و الإقتصادية و السياسية للأفراد و الدول، بل إمتدت لتخلق ساحة جديدة من الحروب غير التقليدية، بعيدا عن ساحات البر و الجو البحر، و هي ساحة الفضاء السيبراني التي توافرت فيها عدة عوامل حفزت بعض الدول و الفاعلين من غير الدول على استخدمها كإحدى أدوات الصراع و التنافس و الهيمنة و الإرهاب غير التقليدي، لدرجة قد تنقل ما يشهده العالم من هجمات إلكترونية مختلفة إلى " حرب سيبرانية" (Cyber War).

و لقد ساعدت عوامل سهولة الإختراق الإلكتروني و انخفاض تكلفة الهجوم و الطبيعة غير المتماثلة للهجمات السيبرانية و صعوبة اكتشاف الفاعل و انتفاء أدلة الإدانة المباشرة و غياب أطر قانونية لتحديد التداعيات و العقوبات، على استخدام هذا الفضاء الجديد في شن هجمات سيبرانية مختلفة، تتراوح بين هجمات ذات طبيعة استراتيجية تطال البنية الحيوية الأساسية، و بين هجمات ذات أهداف عسكرية، و أخرى ذات طبيعة سياسية.

فبرز مفهوم الإرهاب السيبراني، و الذي نتج عن إستخدام التنظيمات الإرهابية و جماعات الجريمة المنظمة، بل و الأفراد العاديين، الفضاء الإلكتروني، لتحقيق أهداف متنوعة، حيث ظهرت مصطلحات جديدة مثل الهاكرز الأفراد، و جماعات المرتزقة السيبرانية، و القراصنة السيبرانيون، و الميليشيات السيبرانية.

و لهذا فقد أحدث ظهور " الحرب السيبرانية " بشكل فعلي على الساحة الأمنية و المعلوماتية منذ منتصف العقد الأول من القرن الحالي نقلة نوعية في مفهوم الحروب التقليدية من حيث الوسائل و الأهداف و النتائج أيضا: فمن حيث الوسائل يتبين أن الحروب دائما ما تتطور بتطور الآليات و الأدوات المستخدمة في شنها، اذ أصبح اختراق قواعد البيانات و المعلومات أو التلاعب بها أو تدميرها من خلال البرامج المعدة لذلك هو العنصر الإستراتيجي في شن الهجمات في عصر الثورة الرقمية، و ذلك بعد أن أضافت الثورة التكنولوجية ساحة جديدة للصراع هي هجمات الفضاء السيبراني (Cyberspace)، و التي تؤذن ببداية ما يمكن تسميته " الحرب السيبرانية "(Cyber War).

و فيما يتعلق بغايات تلك الحرب، فان الخسائر البشرية و المادية لم تعد هي الغاية المباشرة المتوقعة من شن الحروب، و إنما تخطت الهجمات السيبرانية ذلك لغايات أخرى قد يكون من بينها تدمير قواعد البيانات و المعلومات الخاصة بالدول، أو سرقتها و إتاحتها على العلن بغرض إحداث الفضائح السياسية بالشكل الذي يسبب إحراجا للقيادة السياسية لتلك الدول و التأثير على شرعيتها، أو سرقة المعلومات التقنية و الصناعية لدلول بغرض تخريب البنية التحتية الحيوية: وهو الأمر الذي يعكس عمق الخطر الإستراتيجي لتلك الهجمات التي

قد تصل لدرجة الحرب، ما دفع غالبية دول العالم إلى وضع الأمن المعلوماتي و السيبراني في صدارة أولويات الأمن القومي.

و مما لا شكك فيه، فإن تداعيات الصراع في الفضاء السيبراني، وكما تركت تأثيراتها على الأفراد و على الدولي أيضا: فإنها سوف تحدث بمرور الوقت تأثيرات على طبيعة العلاقات الدولية و السياسات العالمية،

وذلك نتاجا لعدة عوامل، أبرزها: إستخدام الهجمات السيبرانية كأداة جديدة لتعزيز الدور الدولي، و إستخدامها كمجال للصراع بين بعض الدول، و صعود أدوار الفاعلين من الدول الصغيرة و المتوسطة و الفاعلين من غير الدول على الساحة الدولية،

و حدوث توتر سياسي و إحتقان دبلوماسي ينتج عن اتهام دولة لأخرى بالتداخل في شؤونها الداخلية عبر الفضاء الإلكتروني و إطلاق سباق تسلح سيبراني بين بعض الدول يتم فيها استخدام وحدات هجوم سيبرانية نظامية أو غير نظامية و تطوير استراتيجيات للدفاع و الردع و الرد السيبراني .

من خلال عرض هذه الدراسة نستنتج أن العصر الذي نعيش فيه بات عصر رقمي تتحكم فيه المعرفة والمعلومات ووسائل الاتصالات، فمن يملك المعرفة يتحكم في كل شيء، وأصبح الفضاء السيبراني واقعي والحروب السيبرانية حقيقة لا مفر منها والتي تعتبر الجيل الخامس من الحروب ويرى الكثير من الأكاديميين أنها نهاية الحروب في المستقبل، وأصبحت الرقمنة هي الصياغة السائدة في العصر الحالي من نقود وحكومات وسيادة السيبرانية وأمن سيبراني ودبلوماسية سيبرانية، كل شيء يتعامل عبر الفضاء الإلكتروني، ولذلك يتوجب على الدول والأفراد الحذر والحيطة عند استخدام البيانات والمعلومات في المجال الإقتراضي، لتجنب الوقوع في مخاطر التصيد الشبكي والهاكرز والجماعات الإرهابية.

قائمـــــة المـــراجـــــع

أولا: المراجع باللغة العربية

- **القرآن الكريم**

1-الكتب:

1- ستيفن لي مايرز، القيصر الجديد،(ترجمه:تيسير نظمي خليل) (المملكة العربية السعودية-الرياض : نشر و توزيع: العبيكان،ط1، 2018).

2- نوران شفيق، **أثر التهديدات الألكترونية على العلاقات الدولية دراسة في أبعاد الأمن الألكتروني**، المكتب العربي للمعارف، القاهرة، 2018.

3- د.فيصل محمد عبد الغفار، **الحرب الإلكترونية**، المنهل، الإمارات العربية المتحدة، 2016.

4- مصطفى يوسف كافي، **الحكومة الإلكترونية في ظل الثورة العلمية التكنولوجية المعاصرة**، دار و مؤسسة رسلان للطباعة و النشر و التوزيع،سوريا – دمشق، 2009 .

5- الدين الجيلالي بوزيد، ماجد الحموي ، **الوسيط في القانون الدولي العام**، دار الشواف- الرياض، 2003

6- فضل الله محمد إسماعيل، **فلسفة القوة: أصولها وتطورها في الفكر السياسي الغربي وآثارها في عالم السياسة** (القاهرة: مكتبة بستان المعرفة، 2006)

7- كليفتون مورجان، **نظرية السياسة الخارجية** (الرياض: منشورات مكتبة الملك فهد الوطنية للنشر، جامع الملك سعود، 2011)

8- أحمد النعيمي، **السياسة الخارجية** (عمان: دار زهران للنشر، 2011)

9- صلاح محمد عبد الحميد، **فن التفاوض والدبلوماسية** (القاهرة: مؤسسة طيبة القاهرة للنشر، 2011)،

10- كارن إن سميث، **الأخلاق والسياسة الخارجية** (تعريب: فاضل جتكر) (الرياض: مكتبة العبيكان، 2005)

11- لويد جنسن، **تفسير السياسة الخارجية** (ترجمة: محمد بن أحمد مفتي، محمد السيد سليم) (الرياض: قسم العلوم السياسية، كلية العلوم الإدارية، جامعة الملك سعود، 1989)

12- أليهاندرو كاسترو أسبين، **إمبراطورية الإرهاب... السياسة الأمريكية العابرة للقارات** (ترجمة: وفيقة إبرهيم) (بيروت: شركة المطبوعات للتزيع والنشر، 2012)

13- فرغلي هارون، **الإرهاب العولميّ وإنهيار الإمبراطورية الأمريكية** (القاهرة: دار الوافي للنشر، 2005)

14- ناعوم تشومسكي، **الإرهاب.. حالة 11 سبتمبر 2001** (الدار البيضاء: مطبعة النجاح الجديدة، 2003)

15- فتوح أبو دهب هيكل، **التدخل الدولي لمكافحة الإرهاب وانعكاساته على السيادة الوطنية** (أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2014)

16- ناعوم تشومسكي، **الإرهاب الدولي... الأسطورة والواقع** (ترجمة: لبنى صبري) (القاهرة: سينا للنشر، 1990)

17- أوليفيه روا، **أوهام 11 أيلول .. المناظرة الإستراتيجية في مواجهة الإرهاب** (ترجمة: حسن الشامي) (الجزائر – بيروت: دار لافارابي، ANEP، 2003)

18- توفيق المديني، **التوتاليتارية الليبرالية الجديدة والحرب على الإرهاب** (دمشق: منشورات اتحاد الكتاب العرب، 2003)، ص. 127.

19- محمد مسعود قيراط، **الإرهاب: دراسة في البرامج الوطنية واستراتيجيات مكافحته.. مقاربة إعلامية** (الرياض: جامعة نايف العربية للعوم الأمنية، 2011)،.

20- عبد الله بلقزيز، **الأمن القومي العربي** القاهرة: الهيئة المصرية العامة للكتاب)، 1989.

21- د. عبد المنعم المشاط، "**الإطار النظري للأمن القومي العربي**" في د. عبد المنعم المشاط (محرر)، **الأمن القومي العربي: أبعاده ومتطلباته** (القاهرة: معهد البحوث والدراسات العربية، 1993)

22- الدين الجيلالي بوزيد، ماجد الحموي ، **الوسيط في القانون الدولي العام** دار الشواف- الرياض، 1424- 2003

23- عبد الله علي عبد الله، **تقنيات الاختراق المادي**، دار البشائر الإسلامية-بيروت،ط1، 2003

24- أسامة سمير حسين،الإحتيال الإلكتروني، **الأسباب و الحلول**، الجنادرية للنشر و التوزيع، ط1، 2011

25- عمر محمد أبو بكر بن يونس: " **الجرائم الناشئة عن استخدام الانترنت الجوانب الموضوعية و الإجرائية**"، (القاهرة: دار النهضة العربية، 2004)

26- رمسيس بهنام:" **المجرم تكوينا و عقيدة**"،(الأسكندرية: منشأة دار المعارف، ب ت)

27- انتصار أنور الغريب:" **أمن الكمبيوتر و القانون**"، (بيروت: دار الراتب الجامعية، 1994)

28- محمد حماد الهيتي، " **جرائم الحاسوب**"،ط1 (عمان: دار المناهج، 2006)

29- مروة زين العابدين صالح، **الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي و القانون الوطني**، مركز الدراسات العربية للنشر و التوزيع، ط1، 2016

30- عبد العالي الديربي، محمد صادق اسمساعيل، **الجرائم الإلكترونية"دراسة قانونية قضائية مقارنة"**، المركز القومي للإصدارت القانونية،ط1، 2012.

31- ايهاب خليفة، **القوة الالكترونية...كيف يمكن ان تدير الدول شؤونها في عصر الانترنت**، القاهرة: العربي للنشر و التوزيع،ط1، 2017.

32- عادل عبد الصادق، **الانترنت والاتصالات، ساحة جديدة للتجسس الدولي**، القاهرة، المركز العربي لأبحاث . الفضاء الالكتروني،2012

33- عادل عبد الصادق، **موقع ويكيليكس وتحدي عالم الاستخبارات الأمريكي**، مركز الأهرام للدراسات،. القاهرة،2010

2_ الملتقيات والمجلات:

1. الهجمات السيبرانية :مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر مجلة المحقق الحلي للعلوم القانونية والسياسية العدد الرابع /السنة الثامنة 2016.

ثانيا: المراجع باللغة الأجنبية

1- Margaret J. Goldstein, Martin Gitlin, **Cyber Attack**, Twenty-First Century Books a division of learner Publishing Group, inc. Minneapolis, Usa 2015.

2- Joseph S. Nye Jr. **The Future of power**. Public Affairs New York, État de New York , 2011.

3- Mark Galeotti, « **The Gerasimov Doctrine and Russian Non-Linear War** », blog In Moscow's Shadows. Analysis and Assessment of Russian Crime and Security, mis en ligne le 6 juillet 2014.

4- Douglas Lovelace, **The Cyber Threat**, Oxford University Press, nov. 2015 – 376 p
5- George Sehwar Zenberger, **Power Politics: A Study of World of Society** (London: Stevens & Sons Limited, 1964).
6- Frank Trager and Philip Kronenberg (eds.), **National Security and American Society** (Kansas: Kansas University Press, 1973)
7- Mitnick, Kevin & William, L. Simon. **Ghost in the Wires**: My Adventures as the World's Most Wanted Hacker. Hachette Book Group, 2011.
8- Verton, Dan. Black Ice: **The Invisible Threat of Cyber-Terrorism**. McGraw-Hill Companies, 2003.
9- Volkman, Ernest. Espionage: **The Greatest Spy Operations of the 20th Century**. John Wiley & Sons, Inc, 1995.
10- Jahankhani, Hamid, et.al. editors. **Handbook of Electronic Security and Digital Forensics**. World Scientific Publishing, 2010
11- Boon, E.Kristen, et.al. editors. Terrorism: Commentary on Security Documents, in "The 2012 Shift in U.S. National Security Strategy: The Context", Vol:131. Oxford University Press, 2013
12- Rosamund, M.Thomas. **Espionage and Secrecy**: **The Official Secrets Acts 1911-1989** of the United Kingdom. Routledge, 1991.
13- Silva, Eugenie, **National Security and Counter intelligence in the Era of Cyber Espionage**, hershey PA, USA, 2015.309p

. ثانيا: مواقع الانترنت

1- https://wikileaks.org/podesta-emails/
2- https://wikileaks.org/dnc-emails/
3- https://wikileaks.org/-Leaks-.html
4- President Obama's Remarks on Securing U.S. Cyber Infrastructure," May 29, 2009, http://www.america.gov/st/texttrans-english/2009/May/2009.
5- James A. Lewis et al, Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, Washington, D.C., CSIS, December 2008, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf . csis-prod.s3.amazonaws.com.
6- Russian Federation, Information Security Doctrine of the Russian Federation, September 2000, http://www.mid.ru/ns-osndoc.nsf/1e5f0de28fe77fdcc3

https://www.independent.co.uk/news/world/americas/donald-trump-election-russia-cia-fbi- comey-clapper-a7480566.html

7- عادل عبد الصادق، الارهاب الالكتروني: القوة في العلاقات الدولية: نمط جديد و تحديات محتلفة، (القاهرة، مركز الأهرام للدراسات السياسية و الإستراتيجية، 2009)

http://coeia.edu.sa/index.php/ar/assurance-awamess/articles/51-forensic-and-computer-crimes/2012/22

8- محمد عبد الله المنشاوي: جرائم الانترنت من منظور شرعي و قانوني

www.minshawi.com

9- اياد قاسم،"واشنطن بوست": الهاكرز الروس يملكون سلاحا سيبرانيا قويا،

https://ar.rt.com/ixn5

10- محمد السعيد:قراصنة الكرملين.. السيطرة على العالم تبدأ من الإنترنت ، مقال منشور على الانترنت (مصدر) تاريخ الدخول : 2018/03/22

https://midan.aljazeera.net/reality/politics/2017/7/12/قراصنة-الكرملين-السيطرة-على-العالم-تبدأ-من-الإنترنت

11- ابراهيم حجازي، كيف إستطاعت المخابرات الروسية إختراق وزارة الدفاع الأمريكية منذ عام 2008

https://www.security4arabs.com/2015/11/29/how-the-russians-hacked-disa/

12- ايهاب شوقي، الحرب السيبرانية...حرب المستقبل المفزعة

http://www.anntv.tv/new/showsubject.aspx?id=101954

13- تايتل برس24 /بغداد،

https://alqabas.com/455104/

14- ليو كليون، ويكيليكس: المخابرات الأمريكية تستخدم أجهزة التلفاز الذكية للتجسس

www.bbc.com/arabic/science-and-tech-39201722

الـفـــهـــرس

الفهـــــــــرس

المضمون | رقم الصفحة

الملخص:

القرصنة الإلكترونية أو المعلوماتيى هي عملية إختراق لأجهزة الحاسوب بطريقة إحترافية، لكنها لا تتوقف عند أجهزة الحاسوب وإنما تشمل كل ما هو مرتب بالشبكات الإلكترونية كالإتصالات و أجهزة الساتيلايت ،و لقد ساعدت عوامل سهولة الإختراق الإلكتروني و انخفاض تكلفة الهجوم و الطبيعة غير المتماثلة للهجمات السيبرانية و صعوبة اكتشاف الفاعل و انتفاء أدلة الإدانة المباشرة و غياب أطر قانونية لتحديد التداعيات و العقوبات، على استخدام هذا الفضاء الجديد في شن هجمات سيبرانية مختلفة و قد أحدث ظهور " الحرب السيبرانية " بشكل فعلي على الساحة الأمنية و المعلوماتية منذ منتصف العقد الأول من القرن الحالي نقلة نوعية في مفهوم الحروب التقليدية من حيث الوسائل و الأهداف و النتائج.

و فيما يتعلق بغايات تلك الحرب قد يكون من بينها تدمير قواعد البيانات و المعلومات الخاصة بالدول، أو سرقتها و إتاحتها على العلن بغرض إحداث الفضائح السياسية، ما دفع غالبية دول العالم إلى وضع الأمن المعلوماتي و السيبراني في صدارة أولويات الأمن القومي.

ولذلك يتوجب على الدول والأفراد الحذر والحيطة عند استخدام البيانات والمعلومات في المجال الإفتراضي، لتجنب الوقوع في مخاطر التصيد الشبكي والهاكرز والجماعات الإرهابية.

<u>الكلمات المفتاحية</u>: أمريكا، روسيا،كوريا، الحروب السيبرانية ، الأمن، الدفاع، السياسة، القرصنة الإلكترونية، الفضاء السيبراني، التهديد، أمن الدول.

<u>Résume</u> :

Le piratage électronique ou informatique est un processus qui pénètre les systèmes informatiques de manière professionnelle, il ne s'arrête pas aux ordinateurs, mais inclut tout ce qui est organisé dans les réseaux électroniques tels que les communications et le satellite.

La facilité des facteurs de pirater électroniques ,le faible coût de l'attaque ,la nature des cyber-attaques asymétriques ,la difficulté de découvrir l'auteur ,l'absence de preuve directe de la condamnation et l'absence de cadres juridiques pour déterminer les conséquences et les sanctions ont contribué à utiliser ce nouvel espace pour lancer diverses attaques informatiques.

L'émergence de « cyber-guerre » a provoqué sur le domaine de la sécurité et de l'informatique depuis le milieu de la première décennie du siècle, un changement de paradigme dans le concept des guerres conventionnelles en termes de moyens , objectifs et résultats.

Le but de cette guerre peut être de détruire ou de voler des bases de données et des informations sur les pays, afin de provoquer des scandales politiques, ce qui a conduit la plupart des pays à placer l'information et la cyber sécurité au sommet des priorités de sécurité nationale.

Les États et les particuliers devraient donc être vigilants dans l'utilisation des données et des informations dans le domaine de la prévention afin d'éviter le risque d'hameçonnage, de pirates et de groupes terroristes

<u>Mots clés</u> : Amérique, Russie, Corée, cyber-guerres, sécurité, défense, politique, cyber-piratage, cyber-espace, menace, sécurité d'état.

<u>Abstract</u> :

Electronic or computer piracy is a process that penetrates computer systems in a professional manner, it does not stop at computers, but includes everything organized in electronic networks such as communications and the satellite.

The ease of electronic hacker factors ,the low cost of attack ,the nature of asymmetric cyber-attacks ,the difficulty of discovering the perpetrator ,the lack of direct evidence of the conviction ,lack of legal frameworks for determine the consequences and sanctions helped to use this new space to launch various computer attacks.

Since the middle of the first decade of the century, the emergence of "cyber-war" has provoked on the field of security and computing a paradigm shift in the concept of conventional wars in terms of means a, objectives and results.

The purpose of this war is to destroy or steal databases and information on countries, in order to provoke political scandals, which has led most countries to place information and cybersecurity at the top of the agenda of national security.

States and individuals should therefore be vigilant in the use of data and information in the field of prevention to avoid the risk of phishing, hackers and terrorist groups.

<u>Key words</u>

The United States, Russia, Korea, Security, defense, politics, role, Cyber Wars, Security, Defense, Politics, Cyber-piracy, Cyberspace, Threat, State Security.